Matrix-based implicit representations of algebraic curves and surfaces and applications

Thang Luu Ba

UNIVERSITÉ DE NICE-SOPHIA ANTIPOLIS - UFR Sciences
École Doctorale Sciences Fondamentales et Appliquées

THÈSE

Pour obtenir le titre de
Docteur en Sciences
de l'UNIVERSITÉ de Nice-Sophia Antipolis

Spécialité : **MATHÉMATIQUES**

présentée et soutenue par

Thang LUU BA

Matrix-based implicit representations of algebraic curves and surfaces and applications

Thèse dirigée par **André GALLIGO** et **Laurent BUSÉ**
soutenue le 12 Juillet 2011

Devant le jury composé de :

M. André Galligo	Professeur, Université de Nice	Directeur
M. Bernard Mourrain	Directeur de Recherche, INRIA Sophia Antipolis	Examinateur
M. Carlos D'Andrea	Professeur, Université de Barcelona	President
M. Gilles Villard	Directeur de Recherche, ENS de Lyon	Rapporteur
M. Laurent Busé	HDR, Chargé de Recherche, INRIA Sophia Antipolis	Co-Directeur
M. Laureano Gonzalez-Vega	Professeur, Université de Cantabria	Rapporteur

Laboratoire J.-A. Dieudonné, Université de Nice
Parc Valrose, 06108 Nice Cedex 2

Project GALAAD, INRIA
2004 Route des Lucioles, 06902 Sophia Antipolis Cedex

Acknowledgments

It would not have been possible to complete this doctoral thesis without the help and support of the kind people around me, to only some of whom it is possible to give particular mention here.

First, I would like to thank my thesis supervisor, Professor André Galligo of UNSA, for what he has supported me during three years of thesis, for his patience, for his good supervision. I would like to thank infinitely my thesis co-supervisor, Laurent Busé, Chargé de recherche à l'INRIA Sophia Antipolis, who has spent a lot of time discussing with me. Moreover, he has helped me to find new directions when I got stuck. Despite my communication problem, he is always patient and keeps calm. Therefore, his attitude has helped me to gain the self-confidence to finish my work.

I am very grateful to Bernard Mourrain, Directeur de recherche and the head of project GALAAD, and Mohamed Elkadi, Maitre de conférence de l'UNSA for their helps and their interesting discussion about my work of thesis. I am also grateful to Grégoire Lecerf, Chargé de recherche à l'École Polytechnique à Palaiseau for his interesting discussion about the software Mathemagix.

Furthermore, I would like to thank Villard Gilles, Directeur de recherche de l'ENS Lyon and Laureano Gonzales-Vega, Professor of Cantabria University, for acceptance to be the reviewers of my thesis. They have given me very precisely and have shown me in details how I could improve the quality of my thesis. I would like to thank Carlos D'Andrea, Professor of Barcelona university and thank again Bernard Mourrain for accepting as the members of my thesis committee.

I would like to acknowledge Government Vietnam and INRIA Sophia Antipolis which gave me the scholarship during my work at France. I also thank the Department of Mathematics, Hanoi National University of Education, particularly associated professors Duong Quoc Viet, Dam Van Nhi, Bui Van Nghi, Phan Doan Thoai for their support since the start of my work in 2002. Thanks to members of the Laboratory J.A. Dieudonnée, EDSFA of Nice University, project GALAAD of INRIA Sophia Antipolis for providing great work environment. Thank Ms Rodrigez, CROUS de Nice, Ms Gallorini, Secretary of EDSFA, for their help during my study at France.

I also would like to thank the Vietnamese friends : Duong - Canh, Dang, Lu, Dung, Chau, Van, Phu-Vui, Yen, Minh, Dan, Huong, Thuan, members of class Mef1-2007 and many others who have shared with me many interesting things during the time at France. I would like to thank the family uncle Phuoc and the family Tinh-François who make my life more harmoniously.

I am very grateful to Angelos (very friendly), my office-mate and my teacher of informatics, Jérôme (very enthusiastic), my office-mate and my teacher of French and Hamad (very

strong), my office-mate, who have shared with me many interesting thing and have helped me a lot during the time at GALAAD project. I also thank to Xu Gang, Médiereg, Elias, Evelyne, Sophie and many other friends in GALAAD team and Laboratory J.A. Dieudonné who have encouraged me during my thesis. I will never forget the happy time I have shared with my friends at GALAAD team.

I owe my deepest gratitude to my parents, my parents in law, my sister in law and the family of my brothers who always encourage me to finish my thesis.

Finally, I am extremely grateful to my wife Đỗ Thị Quỳnh Nga and my son Luu Đỗ Tuấn who have given me their personal support and greatest patience at all time.

Contents

Introduction

Rational algebraic curves and surfaces can be described in some different ways, the most common being parametric and implicit representations. Parametric representations describe the geometric object as the closed image of a rational map and implicit representations describe it as the zero set of a polynomial equation. Both representations have a wide range of applications in Computer Aided Geometric Design (CAGD) and Geometric Modeling. A parametric representation is much easier for drawing a surface but more difficult for checking if a point lies on a surface whereas an implicit representation is more difficult for drawing a surface but much easier for checking if a point lies on a surface. In recent years, several authors (for example [1–10]) proposed a new representation of algebraic hypersurfaces by means of a matrix. These representation matrices can be seen as a bridge between the parametric representation of this hypersurface and its implicit representation. Let us give a brief overview.

Suppose given a hypersurface $\mathcal{H}$ of $\mathbb{P}^n$ defined as the closed image of a rational map

$$\begin{array}{rcl} \mathbb{P}^{n-1}_{\mathbb{K}} & \xrightarrow{\phi} & \mathbb{P}^{n}_{\mathbb{K}} \\ (x_1 : x_2 : \ldots : x_n) & \mapsto & (f_1(x_1, \ldots, x_n) : \ldots : f_{n+1}(x_1, \ldots, x_n)) \end{array}$$

where $\mathbb{K}$ is an algebraic closed field and $f_1, \ldots, f_{n+1} \in \mathbb{K}[X_1, \ldots, X_n]$ are homogeneous polynomials of the same degree $d \geq 1$. The implicitization problem consists in the determination of an implicit equation $H(T_1, ..., T_{n+1})$ of this hypersurface. Notice that H is a homogeneous polynomial of $\mathbb{K}[T_1, \ldots, T_{n+1}]$ whose degree is equal to the degree of the hypersuface $\mathcal{H}$. From an algebraic point of view, the map ϕ corresponds to the ring morphism

$$\begin{array}{rcl} h : \mathbb{K}[T_1, \ldots, T_{n+1}] & \rightarrow & \mathbb{K}[X_1, \ldots, X_n] \\ P(T_1, \ldots, T_{n+1}) & \mapsto & P(f_1, \ldots, f_{n+1}) \end{array}$$

whose kernel $\ker(h)$ is a principal ideal of $\mathbb{K}[T_1, \ldots, T_{n+1}]$ generated by an implicit equation of $\mathcal{H}$. In the recent years, several authors, see for example [2, 4, 7, 9, 10], approached the implicitization problem by substituting to the homogeneous polynomial $H(T_1, ..., T_{n+1})$, a classical representation of the hypersurface $\mathcal{H}$, a matrix with its entries in $\mathbb{K}[T_1, \ldots, T_{n+1}]$. This matrix is much simpler to calculate and more compact. However, it becomes necessary to develop new algorithms to manipulate these new representations. This is one of the main purpose of this thesis work.

Consider a rational space curve defined as the closed image of a rational map

$$\begin{array}{rcl} \mathbb{P}^{1}_{\mathbb{K}} & \xrightarrow{\phi} & \mathbb{P}^{n}_{\mathbb{K}} \\ (s : t) & \mapsto & (f_1(s, t) : \ldots : f_{n+1}(s, t)) \end{array}$$

where $\mathbb{K}$ is an algebraic closed field and $f_1, \ldots, f_{n+1} \in \mathbb{K}[s,t]$ are homogeneous polynomials of the same degree $d \geq 1$. An implicit representation of $\mathcal{C}$ in $\mathbb{P}^n_{\mathbb{K}}$ is the *defining ideal* of $\mathcal{C}$, that we will denote by $\mathfrak{I}_{\mathcal{C}}$. 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, $\mathfrak{I}_{\mathcal{C}}$ is the set of polynomials $P \in \mathbb{K}[x_0, \ldots, x_n]$ satisfying 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 $\mathfrak{I}_{\mathcal{C}}$ provides a representation of $\mathcal{C}$ since we have, in terms of algebraic varieties,

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

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

In this thesis, we propose a new matrix representation of rational curves in the projective space of abitrary dimension and illustrate the advantages of this representation by addressing some important problems of Computer Aided Geometric Design: The curve/curve intersection problem, the point-on-curve, inversion problems and the computation of singularities.

Let us sum up briefly the contents of each chapter.

In the first chapter, we will focus on the construction of matrix representations of algebraic curves and surfaces that are given by a parameterization. This has been studied with details in the case of hypersurfaces parameterized by a projective space (see for instance [4,5,7,10] and reference therein) . The results that are obtained are very general and based on the use of theoretical tools from commutative and homological algebra. However, the case of rational curves in the projective space of arbitrary dimension is very different because a single implicit equation is not enough to describe this curve, several equations are necessary. The determination of these equations in good shape and in small number is a difficult problem (see, for example, [12–14]). In this chapter, we propose new 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 projective 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 which has been introduced in [15].

In the second chapter, we will show how to use matrix-based implicit representations of rational curves and surfaces to solve the curve/curve and curve/surface intersection problems, the point-on-curve and inversion problems, the detection of singularities. To solve the intersection between algebraic varieties, there are several methods and approaches which have been developed. Some of them are based on matrix representations of the objects that allow to transform the computation of the intersection locus into generalized eigencomputations (see for instance [8, 16, 17] and the references therein). As far as we know, all these methods have only been developed for *square* matrix representations. One of the main contribution of this chapter is to show that similar algorithms can be implemented even if the matrix representation used are non square matrices. These non square representation matrices appear under much less restrictive hypothesis, notably regarding what is called base

points. Moreover, they are much easier to compute than square representation matrices when they exist. To solve the curve/curve and curve/surface intersection problems, we will develop an algorithm that consists in two main steps. The first one is the computation of a matrix representation of the curve and surface from its parameterization. After mixing this matrix representation of the surface with the parameterization of the curve, the second step consists of a matrix reduction and some eigencomputations. As a particularity of our method, the first step can be performed by symbolic, exact computations and the second step, by numerical computations. The point-on-curve and inversion problems, the detection of singularities have been considered recently in [13, 14, 18] with methods based on a set of equations that are built from a μ-basis of the parameterization. We will show 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. In this chapter, we also show how it is possible to hande curves in a projective space of higher dimension than 3 for applications in CAGD. Hereafter, we consider the problem of computing lines of intersection between two ruled surfaces. 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 [19, 20] to compute the complete intersection locus between two ruled surfaces.

In the third chapter, we extend the approach developed in the second chapter for decomposing the intersection locus between two parameterized surfaces. Unlike the case of solving the curve/curve and curve/surface intersection problems, solving the surface/surface intersection problem by means of matrix representation is much more complicated, mainly because it amounts to compute the generalized eigenvalues of a bivariate pencil of matrices. In this chapter, we propose an algorithm for computing the one dimensional and zero dimensional eigenvalue locus of the bivariate pencil of matrices so that we can obtain the defining equations of the intersection curve of two rational surfaces and also its isolated points. The ideas and techniques in this chapter have been developed in the second chapter and [8, 21, 22].

The last chapter is not directly related to the previous ones and targets different applications. We will focus on using some theoretical tools from commutative algebra so-called syzygies, Hilbert function, Gröbner basis, generic initial ideal to solve a problem posed by Von sur Gathen and all [23]: suppose given a family of generic univariate polynomials $f := (f_0, f_1, ..., f_s)$, contruct an algorithm to find polynomial perturbation $u := (u_0, u_1, ..., u_s)$ with "small" degree such that the GCD (greatest common divisor) of the perturbed family $f + u := (f_0 + u_0, f_1 + u_1, ..., f_s + u_s)$ has "large" degree. We propose an algorithm that solves this problem in polynomial time under a generic condition generalizing the normal degree sequence used in [23] in the case $s = 1$.

At the end of this thesis work, we provide an appendix to illustrate how to compute a matrix representation of curves and surfaces, μ-basis, generalized eigenvalues, polynomial equation, intersection points of curve/surface and curve/curve, singular points of curve with the computer algebra system *Mathemagix* [24] by the package *matrixrepresentation* which is developed at INRIA in the project GALAAD. This work has been conduced during this thesis in parallel of the theoretical developvements. All these programs are included in the current distribution of Mathemagix, in the shape module *mmx/shape/mmx /matrixrepresentation* or at *http://www-sop.inria.fr/members/Luu.Ba_Thang/*

Chapter 1

Matrix-based implicit representations of rational algebraic curves and surfaces

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

In this chapter, we first begin by recalling some known methods to build a matrix that represents a rational hypersurface, particularly rational curves in the plane and rational surfaces in the space.

In the second part of this chapter we introduce and study a new implicit representation of rational curves in a projective space of arbitrary dimension. To motive this problem, we give a brief overview. 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 example, [12], [13] and [14]). In this thesis work, we propose new implicit representation 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 1.2.1. The new matrix-based representations of rational curves which we propose will be exposed in Section 1.2. The results in this chapter are joint work with Laurent Busé and have been published in [25]

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

1.1 Matrix-based implicit representations of rational hypersufaces

Given a parametrized algebraic hypersurface, the aim of this part is to report on known results about building a matrix that *represents* this hypersurface. The entries of this matrix are linear in the space of implicit variables. In order to clarify our approach and put it in perspective, we begin with the more simple case of parametrized algebraic plane curves.

1.1.1 Rational plane algebraic curves

Suppose given a parametrization

$$\begin{array}{rcl} \mathbb{P}^1_{\mathbb{K}} & \xrightarrow{\phi} & \mathbb{P}^2_{\mathbb{K}} \\ (s:t) & \mapsto & (f_1:f_2:f_3)(s:t) \end{array}$$

of a plane algebraic curve $\mathcal{C}$ in $\mathbb{P}^2$. We set $d := \deg(f_i) \geq 1$, $i = 1,2,3$ and denote by x, y, z the homogeneous coordinates of the projective plane $\mathbb{P}^2_{\mathbb{K}}$. The implicit equation of $\mathcal{C}$ is a homogeneous polynomial $C \in \mathbb{K}[x,y,z]$ satisfying the property $C(f_1,f_2,f_3) \equiv 0$ and with the smallest possible degree (notice that C is actually defined up to multiplication by a nonzero element of $\mathbb{K}$). It is well known that

$$\deg(\phi)\deg(C) = d - \deg(\gcd(f_1,f_2,f_3))$$

where $\deg(\phi)$ is the degree of the parametrization ϕ. Roughly speaking, the integer $\deg(\phi)$ measures the number of times the curve $\mathcal{C}$ is drawn by the parametrization ϕ. For simplicity, from now on we will assume that $\gcd(f_1,f_2,f_3) \in \mathbb{K}\backslash\{0\}$, that is to say that the parametrization ϕ is defined everywhere. Notice that the last condition is not restrictive because we can obtain it by dividing for each $f_i, i = 1,2,3$ by $\gcd(f_1,f_2,f_3)$.

Now, we recall two types of method to compute the implicit equation of the curve $\mathcal{C}$. The first one is based on a resultant computation. Denote by $\mathrm{Sylv}(f_1 - T_1 f_3, f_2 - T_2 f_3)$ the well-known Sylvester's matrix of two polynomial $f_1 - T_1 f_3$ and $f_2 - T_2 f_3$ in variables s and t. We can obtain the implicit equation of the curve $\mathcal{C}$ as the determinant of $\mathrm{Sylv}(f_1 - T_1 f_3, f_2 - T_2 f_3)$ i.e. we have

$$\mathrm{Res}(f_1 - T_1 f_3, f_2 - T_2 f_3) = \det \mathrm{Sylv}(f_1 - T_1 f_3, f_2 - T_2 f_3) = C(T_1,T_2,1)^{\deg(\phi)},$$

where Res denotes the classical resultant of two homogeneous polynomial in $\mathbb{P}^1_{\mathbb{K}}$. Another matrix formulation is known to compute such a resultant, the Bezout's matrix which is of smaller size. If $P(s,t)$ and $Q(s,t)$ are two homogeneous polynomials of the same degree d, then the Bezout's matrix $\mathrm{Bez}(P,Q)$ is the matrix $(b_{i,j})_{0 \leq i \leq j \leq d-1}$ where $b_{i,j}$'s are the coefficients of the decomposition

$$\frac{P(s,1)Q(t,1) - P(t,1)Q(s,1)}{s-t} = \sum_{0 \leq i \leq j \leq d-1} b_{i,j} s^i t^j.$$

Since $\det \mathrm{Bez}(P,Q) = \mathrm{Res}(P,Q)$, we have

$$\det(\mathrm{Bez}(f_1 - T_1 f_3, f_2 - T_2 f_3)) = C(T_1,T_2,1)^{\deg(\phi)}.$$

This result shows that the matrices $\mathrm{Sylv}(f_1 - T_1 f_3, f_2 - T_2 f_3)$ and $\mathrm{Bez}(f_1 - T_1 f_3, f_2 - T_2 f_3)$ can be seen as an implicit representations of the curve $\mathcal{C}$. They are actually both special cases of a method so-called *moving line* which was introduced by Sederbeg and Chen in [7]. We can build a collection of matrices that are associated to the parametrization ϕ as follows. For all non negative integer ν, consider the set $\mathcal{L}_\nu$ of polynomials of the form

$$a_1(s,t)x + a_2(s,t)y + a_3(s,t)z \in \mathbb{K}[s,t][x,y,z]$$

such that

- $a_i(s,t) \in \mathbb{K}[s,t]$ is homogeneous of degree ν for all $i = 1,2,3$ and
- $\sum_{i=1}^{3} a_i(s,t) f_i(s,t) \equiv 0$ in $\mathbb{K}[s,t]$.

By definition, it is clear that $\mathcal{L}_\nu$ is a $\mathbb{K}$-vector space and that a basis, say $L^{(1)}, \ldots, L^{(n_\nu)}$, of $\mathcal{L}_\nu$ can be computed by solving a single linear system with indeterminates the coefficients of the polynomials $a_i(s,t)$, $i = 1,2,3$. The matrix $\mathtt{M}(\phi)_\nu$ is the matrix of coefficients of $L^{(1)}, \ldots, L^{(n_\nu)}$ as homogeneous polynomials of degree ν in the variables s,t. In other words, we have the equality

$$\left[\begin{array}{cccc} s^\nu & s^{\nu-1}t & \cdots & t^\nu \end{array}\right] \mathtt{M}(\phi)_\nu = \left[\begin{array}{cccc} L^{(1)} & L^{(2)} & \cdots & L^{(n_\nu)} \end{array}\right]$$

The entries of $\mathtt{M}(\phi)_\nu$ are linear forms in $\mathbb{K}[x,y,z]$. As the integer ν varies, we have the following picture for the size of the matrix $\mathtt{M}(\phi)_\nu$:

- if $0 \leq \nu \leq d-2$ the number n_ν of columns is strictly less than $\nu + 1$ which is the number of rows,
- if $\nu = d-1$ then $\mathtt{M}(\phi)_{d-1}$ is a square matrix of size d,
- if $\nu \geq d$ the number n_ν of columns is strictly bigger than $\nu + 1$ which is the number of rows.

Proposition 1 ([5]). *For all $\nu \geq d-1$ the two following properties hold :*

- *the GCD of the minors of (maximum) size $\nu+1$ of $\mathtt{M}(\phi)_\nu$ is equal to $C(x,y,z)^{\deg(\phi)}$ up to multiplication by a nonzero element in $\mathbb{K}$,*
- *$\mathtt{M}(\phi)_\nu$ is generically full rank and its rank drops exactly on the curve $\mathcal{C}$.*

This result shows that all the matrices $\mathtt{M}(\phi)_\nu$ such that $\nu \geq d-1$, can serve as an implicit representation of the curve $\mathcal{C}$ in the same way as the implicit equation $C(x,y,z)$ is an implicit representation of the curve $\mathcal{C}$.

The matrix $\mathtt{M}(\phi)_{d-1}$ is particularly interesting because it is the smallest matrix representing the curve $\mathcal{C}$ and especially because it is a square matrix, which implies that

$$\det(\mathtt{M}(\phi)_{d-1}) = c.C(x,y,z)^{\deg(\phi)}$$

where $c \in \mathbb{K} \setminus \{0\}$. This matrix goes back, as far as we know, to the work [7] and has been widely exploited since then by the community of Geometric Modeling and Computer Aided Geometric Design.

It is natural to wonder if such an approach can be carried out to the case of parametrized algebraic surfaces. As we will see, most of the above results hold in this case with much more involved details and some suitable hypothesis. However, it turns out that a matrix similar to the matrix $\mathtt{M}(\phi)_{d-1}$ rarely exists. Therefore, in order to keep a square matrix it is necessary to introduce quadratic syzygies, or higher order syzygies; see for instance [2, 3, 26]. In the sequel, we will stick to the case of linear syzygies because of their simplicity and generality, even if we will not get square matrices in general.

1.1.2 Rational algebraic surfaces

Suppose given a parametrization

$$\begin{array}{rcl} \mathbb{P}^2_{\mathbb{K}} & \xrightarrow{\phi} & \mathbb{P}^3_{\mathbb{K}} \\ (s:t:u) & \mapsto & (f_1:f_2:f_3:f_4)(s,t,u) \end{array}$$

of a surface $\mathbf{S}$ such that $\gcd(f_1,\ldots,f_4) \in \mathbb{K}\setminus\{0\}$. Set $d := \deg(f_i) \geq 1$, $i = 1,2,3,4$ and denote by $S(x,y,z,w) \in \mathbb{K}[x,y,z,w]$ the implicit equation of $\mathbf{S}$ which is defined up to multiplication by a nonzero element in $\mathbb{K}$. Similarly to the case of parametrized plane curves, there also exists a degree formula that asserts that the quantity $\deg(\mathbf{S})\deg(\phi)$ is equal to d^2 minus the number of common roots of f_1, f_2, f_3, f_4 in $\mathbb{P}^2$ counted with suitable multiplicities (see for instance [5, Theorem 2.5] for more details). As for curve implicitization, some types of method have been developed to solve the surface implicitization problem: Method based on resultant computations, the method called *moving surface* and the method based on *approximation complex*. We begin with the first which is also the oldest one. If there is no base points (i.e a point in $\mathbb{P}^2_{\mathbb{K}}$ is called a *base point* of the parametrization ϕ if it is a common root of the polynomials $f_1,\ldots,f_4$), it is known that

$$\mathrm{Res}(f_1 - T_1 f_4, f_2 - T_2 f_4, f_3 - T_3 f_4) = S(T_1,T_2,T_3,1)^{\deg(\phi)},$$

where Res denotes the classical resultant of three homogeneous polynomial in $\mathbb{P}^2_{\mathbb{K}}$. This resultant can be computed with the well-known Macaulay's matrices but this involves $\gcd$ computations since the determinant of each Macaulay's matrix give only a multiple of this resultant. To avoid these $\gcd$ computations, the following method has been proposed in some sens, it contains this resultat computation. We build a collection of matrices associated to the parametrization ϕ as follows. For all non negative integer ν, consider the set $\mathcal{L}_\nu$ of polynomials of the form

$$a_1(s,t,u)x + a_2(s,t,u)y + a_3(s,t,u)z + a_4(s,t,u)w$$

such that

- $a_i(s,t,u) \in \mathbb{K}[s,t,u]$ is homogeneous of degree ν for all $i = 1,\ldots,4$,
- $\sum_{i=1}^4 a_i(s,t,u)f_i(s,t,u) \equiv 0$ in $\mathbb{K}[s,t,u]$.

This set is a $\mathbb{K}$-vector space; denote by $L^{(1)},\ldots,L^{(n_\nu)}$ a basis of it that can be computed by solving a single linear system. Then, define the matrix $\mathtt{M}(\phi)_\nu$ by the equality

$$\left[\begin{array}{cccc} s^\nu & s^{\nu-1}t & \cdots & u^\nu \end{array}\right] \mathtt{M}(\phi)_\nu = \left[\begin{array}{cccc} L^{(1)} & L^{(2)} & \cdots & L^{(n_\nu)} \end{array}\right]$$

The method that we build $\mathtt{M}(\phi)_\nu$ is called *moving planes* of degree ν following the surfaces $\mathbf{S}$ which also has been introduced in [7]. From a computational point of view, we can see that this matrix can be taken as a *representation* of the surfaces $\mathbf{S}$, replacing an expanded implicit equation (even if it is generally non-square). For instance, to test if a given point $P := (x_0 : y_0 : z_0 : w_0) \in \mathbb{P}^3_{\mathbb{K}}$ is in the surface $\mathbf{S}$, we just have to substitute x, y, z, w respectively by x_0, y_0, z_0, w_0 in $\mathtt{M}(\phi)_\nu$ and check its rank. P is on $\mathbf{S}$ if and only if the rank is drop.

In a similar way, a moving quadratic of the degree ν following the surface is a polynomial of the form

$$a_{1,1}(s,t,u)T_1^2 + a_{1,2}(s,t,u)T_1T_2 + \cdots + a_{4,4}(s,t,u)T_4^2,$$

where $a_{i,j}(s,t,u), 1 \leq i \leq j \leq 4$ are homogeneous polynomial in $\mathbb{K}[s,t,u]_\nu$, such that it vanishes if we replace T_i by f_i. Choosing d moving planes $L_1, \ldots, L_d$ and $l = (d^2-d)/2$ moving quadrics $Q_1, \ldots, Q_l$ of degree $d-1$ which follow the surface $\mathbf{S}$, we can construct a square matrix $\mathbf{M}$, corresponding to the $\mathbb{K}[T]$-module map (where $\mathbb{K}[T]$ denotes $\mathbb{K}[T_1, T_2, T_3, T_4]$)

$$\begin{array}{rcl} (\oplus_{i=1}^d \mathbb{K}[T]) \oplus (\oplus_{j=1}^l \mathbb{K}[T]) & \to & (\mathbb{K}[s,t,u]_{d-1}) \otimes_{\mathbb{K}} \mathbb{K}[T] \\ (p_1, \ldots, p_d, q_1, \ldots, q_n) & \mapsto & \sum_{i=1}^d p_i L_i + \sum_{j=1}^l q_i Q_i \end{array}$$

It can be shown that it is always possible to choose $L_1, \ldots, L_d$ and $Q_1, \ldots, Q_l$ so that $\det(M)$ is non-zero and then equal $S(x,y,z,w)^{\deg(\phi)}$(see [27]). This method is way improved in [2].

In the recent years, Busé, Jouanolou and Chadin in [5, 28] have developed a method based on a method, called *approximation complexes* introduced by Simis and Vasconcelos in [29,30], for solving the implicitization problem of a hypersurfaces $\mathcal{H}$ of $\mathbb{P}^n$ (hence a curve and surface) defined as the closed image of a rational map

$$\begin{array}{rcl} \mathbb{P}^{n-1}_{\mathbb{K}} & \xrightarrow{\phi} & \mathbb{P}^n_{\mathbb{K}} \\ (x_1 : x_2 : \ldots : x_n) & \mapsto & (f_1(x_1, \ldots, x_n) : \ldots : f_{n+1}(x_1, \ldots, x_n)) \end{array}$$

in the case where the base points are isolated and locally a complete intersection, without any additional hypothesis. Comparing with the method of moving surface, the resultant-based method, this method is more general since both preceding method somes times failed in this situation (for more detail see [5]). An algorithm for implicitizing rational hypersurface following the method *approximation complexes* has been described and improved in [4, 5]. For more detail, we give an explicit description for the method *approximation complexes* in the case $n = 3$. Notice that this description has given in [4, 5].

We denote by A the polynomial $\mathbb{K}[s,t,u]$ which is naturally graded by $\deg(s) = \deg(t) = \deg(u) = 1$. From the polynomial f_1, f_2, f_3, f_4 of the parametrization ϕ, we build the well-known graded Koszul complex (see for instance [31]) of a sequence (f_1, f_2, f_3, f_4) in A (notation $[-n]$ stand for the degree shift n in A):

$$0 \to A[-4d] \xrightarrow{d_4} A[-3d] \xrightarrow{d_3} A[-2d] \xrightarrow{d_2} A[-d] \xrightarrow{d_1} A \tag{1.1.1}$$

where the differentials $d_i (i = 1, 2, 3, 4)$ are given by

$$d_4 = \begin{pmatrix} -f_4 \\ f_3 \\ -f_2 \\ f_1 \end{pmatrix}, d_3 = \begin{pmatrix} f_3 & f_4 & 0 & 0 \\ -f_2 & 0 & f_4 & 0 \\ f_1 & 0 & 0 & f_4 \\ 0 & -f_2 & -f_3 & 0 \\ 0 & f_1 & 0 & -f_2 \\ 0 & 0 & f_1 & f_2 \end{pmatrix},$$

$$d_2 = \begin{pmatrix} -f_2 & -f_3 & 0 & -f_4 & 0 & 0 \\ f_1 & 0 & -f_2 & 0 & -f_4 & 0 \\ 0 & f_1 & f_2 & 0 & 0 & -f_4 \\ 0 & 0 & f_1 & f_2 & f_3 & \end{pmatrix}, d_1 = (f_1, f_2, f_3, f_4).$$

Tensoring the complex (1.1.1) by $A[x, y, z, w]$ over A, we obtain the complex denote by $(K_\bullet(f_1, f_2, f_3, f_4), u_\bullet)$ which is of the form

$$0 \to A[x, y, z, w][-4d] \xrightarrow{u_4} A[x, y, z, w][-3d] \xrightarrow{u_3} A[x, y, z, w][-2d] \xrightarrow{u_2} A[x, y, z, w][-d]$$
$$\xrightarrow{u_1} A[x, y, z, w]$$

where the matrices of the differential d_i and u_i are the same. Set $\deg(x) = \deg(y) = \deg(z) = \deg(w) = 1$, we build the bi-graded Koszul complex on $A[x, y, z, w]$ of a sequence (x, y, z, w) denote by $(K_\bullet(x, y, z, w), v_\bullet)$ which is of the form

$$0 \to A[x, y, z, w][-4] \xrightarrow{v_4} A[x, y, z, w][-3] \xrightarrow{v_3} A[x, y, z, w][-2] \xrightarrow{v_2} A[x, y, z, w][-1]$$
$$\xrightarrow{v_1} A[x, y, z, w]$$

and the matrices of its differentials are obtained from the matrices of the differentials (1.1.1) by replacing f_1, f_2, f_3, f_4 by x, y, z, w respectively. From the complex Koszul $(K_\bullet(f_1, f_2, f_3, f_4), u_\bullet)$ and $(K_\bullet(x, y, z, w), v_\bullet)$, we can build the complex $\mathcal{Z}_\bullet$ so-called *approximation complex* by defining $\mathcal{Z}_i := \ker(d_i) \otimes_A A[x, y, z, w]$ for $i = 0, 1, 2, 3, 4$ (where $d_0 : A \to 0$). They are bi-graded $A[x, y, z, w]$ - modules. For $i = 1, 2, 3$, we have $u_i \circ v_{i+1} + v_i \circ u_{i+1} = 0$, thus we obtain the bi-graded complex

$$(\mathcal{Z}_\bullet, v_\bullet) : 0 \to \mathcal{Z}_3(-3) \xrightarrow{v_3} \mathcal{Z}_2(-2) \xrightarrow{v_2} \mathcal{Z}_1(-1) \xrightarrow{v_1} \mathcal{Z}_0 = A[x, y, z, w].$$

Remark 2. An element $(g_1, g_2, g_3, g_4) \in \mathcal{Z}_{1[\nu]}$ is a moving plane of degree ν following the surface S. So the matrix of the surjective map

$$\begin{array}{rcl} \mathcal{Z}_{1[\nu]}(-1) & \xrightarrow{v_1} & A_\nu[x, y, z, w] \\ (g_1, g_2, g_3, g_4) & \mapsto & xg_1 + yg_2 + zg_3 + wg_4 \end{array}$$

is exact the matrix $\mathtt{M}(\phi)_\nu$ which we describe in the method moving surfaces.

Before giving the main properties of this collection of matrices, we need the following

Definition 3. A matrix $\mathtt{M}(\phi)$ with entries in $\mathbb{K}[x, y, z, w]$ is said to be a representation of a given homogeneous polynomial $P \in \mathbb{K}[x, y, z, w]$ if

i) $\mathtt{M}(\phi)$ is generically full rank,

ii) the rank of $\mathtt{M}(\phi)$ drops exactly on the surface of equation $P = 0$,

Recall that a point in $\mathbb{P}^2_{\mathbb{K}}$ is called a *base point* of the parametrization ϕ if it is a common root of the polynomials $f_1, \ldots, f_4$. It is said to be *locally a complete intersection* if it can be locally generated by two equations, and said to be *locally an almost complete intersection* if it can be locally generated by three equations.

Proposition 4 ([4, 10])**.** *For all integer $\nu \geq 2(d-1)$ we have:*

- *if the base points are local complete intersections then $\mathtt{M}(\phi)_\nu$ represents $S^{\deg(\phi)}$,*
- *if the base points are almost local complete intersections then $\mathtt{M}(\phi)_\nu$ represents*

$$S^{\deg(\phi)} \times \prod_{\mathbf{p} \in V(f_1,\ldots,f_4) \subset \mathbb{P}^2_{\mathbb{K}}} L_{\mathbf{p}}(x,y,z,w)^{e_{\mathbf{p}}-d_{\mathbf{p}}}$$

where $L_{\mathbf{p}}(x,y,z,w)$ are linear forms.

Remark 5. It is possible to improve the bound $2(d-1)$ by taking into account the geometry of the base points; we refer the reader to [4] for more details. For instance, if there exists at least one common root to $f_1, \ldots, f_4$ in $\mathbb{P}^2$ then the above proposition is true for all $\nu \geq 2(d-1)-1$. Also, mentioned that the linear forms $L_{\mathbf{p}}(x, \ldots, w)$ can be determined by computations of syzygies in $\mathbb{K}[s,t,u]$; see [10].

Although we are dealing with surfaces parametrized by the projective plane, it is important to mention that the above results still hold for surfaces parametrized by the product of two projective lines, or more generally by a toric variety. We refer the interested reader to [1,9,32] for these extensions and also, a recent improvement of moving quadratics in [6]

1.2 Matrix-based implicit representations of rational algebraic curves

In the previous part, we recalled an implicit representation of rational plane curve. In this part, we introduce and study a new implicit representation of a rational curve in a projective space of arbitrary dimension. The results in this part have been published in [25]

1.2.1 The defining ideal of a rational curve and μ-bases

Let $f_0, f_1, \ldots, f_n$ be n 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

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

The image of ϕ is an algebraic curve $\mathcal{C}$ in $\mathbb{P}^n_{\mathbb{K}}$ which is called a *rational* curve. The degree of $\mathcal{C}$ is the number of intersection points counted properly between $\mathcal{C}$ and any hyperplane in $\mathbb{P}^n_{\mathbb{K}}$ not containing $\mathcal{C}$. 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 $\mathcal{C}$ through the equation

$$\deg(\mathcal{C})\deg(\phi) = d.$$

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 $\mathcal{C}$ via ϕ.

1.2.2 The defining ideal of a rational curve

The parameterization ϕ is a very practical representation of $\mathcal{C}$ and it is widely used in CAGD. However, for many problems it is useful to have an implicit representation of $\mathcal{C}$, 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 $\mathcal{C}$ in $\mathbb{P}^n_{\mathbb{K}}$ is the *defining ideal* of $\mathcal{C}$, that we will denote by $\mathfrak{I}_{\mathcal{C}}$. By definition, it is the kernel of the ring morphism

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

In other terms, $\mathfrak{I}_{\mathcal{C}}$ 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 $\mathfrak{I}_{\mathcal{C}}$ provides a representation of $\mathcal{C}$ since we have, in terms of algebraic varieties

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

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

1.2.3 μ-basis of a rational curve

The concept of a μ-basis has been introduced in [15]. It can be seen as a bridge between the parametric representation ϕ of $\mathcal{C}$ and its implicit representation $\mathfrak{I}_{\mathcal{C}}$. 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 [33, §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 exists non-negative integers $\mu_1, \ldots, \mu_n$ and n vectors of polynomials

$$(u_{i,0}(s,t), u_{i,1}(s,t), \ldots, u_{i,n}(s,t)) \in \mathrm{Syz}(\mathbf{f}) \subset \mathbb{K}[s,t]^{n+1} \ \ (i = 1, \ldots, n) \tag{1.2.1}$$

such that

- for all $i \in \{1, \ldots, n\}$, $j \in \{0, \ldots, n\}$, $u_{i,j}(s,t)$ is a homogeneous polynomial in $\mathbb{K}[s,t]$ of degree $\mu_i \geq 0$,
- the n vectors in (1.2.1) form a $\mathbb{K}[s,t]$-basis of $\mathrm{Syz}(\mathbf{f})$,
- $\sum_{i=1}^{n} \mu_i = d$,
- For all $j \in \{0, \ldots, n\}$, the determinant of the matrix obtained by deleting the column $(u_{i,j})_{i=1,\ldots,n}$ from the matrix

$$M(s,t) := \begin{pmatrix} u_{1,0}(s,t) & u_{1,1}(s,t) & \ldots & u_{1,n}(s,t) \\ u_{2,0}(s,t) & u_{2,1}(s,t) & \ldots & u_{2,n}(s,t) \\ \ldots & \ldots & \ldots & \ldots \\ u_{n,0}(s,t) & u_{n,1}(s,t) & \ldots & u_{n,n+1}(s,t) \end{pmatrix} \tag{1.2.2}$$

  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 (1.2.1) that satisfy the above properties is called a μ-basis of the parametrization ϕ. It is important to notice that a μ-basis is far from being unique, but the collection of integers $(\mu_1, \mu_2, \ldots, \mu_n)$ is unique if we order it. Therefore, in the sequel we will always assume that a μ-basis is ordered so that $0 \leq \mu_1 \leq \mu_2 \leq \cdots \leq \mu_n$. We refer the interested reader to [13] for more details on the topic of μ-basis.

1.2.4 Projection of the graph of ϕ

Here is an important property of a μ-basis as a tool for the representation of the curve $\mathcal{C}$. Recall that $M(s,t)$ denotes the matrix (1.2.2) built from a μ-basis of ϕ.

Lemma 6. *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*

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

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 $i = 1, \ldots, n$ set

$$u_i(s,t,x_0,x_1,\ldots,x_n) = \sum_{j=0}^{n} u_{i,j}(s,t)x_j \in \mathbb{K}[s,t,x_0,\ldots,x_n]. \tag{1.2.3}$$

An immediate consequence of Lemma 6 is that the algebraic variety W defined by the zero locus of the μ-basis, i.e.

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

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

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

sends W on $\mathcal{C}$; we have $\pi(W) = \mathcal{C}$ (for more detail, see [34, Lecture 2]). 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 $A := \mathbb{K}[x_0, \ldots, x_n]$, so that $\mathbb{K}[s, t, x_0, \ldots, x_n] = A[s, t]$, the ideal $I := (u_1, \ldots, u_n)$ of $A[s, t]$ and consider its *resultant ideal* (also called the projective elimination ideal in [35, 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 7 ([5, Corollary 3.8])**.** *With the above notation, we have $\mathfrak{A} = \mathfrak{I}_{\mathcal{C}}$ as ideals of A.*

In the next section, we will take advantage of this proposition to produce a matrix-based representation of $\mathcal{C}$. 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 8. *For all integer $\nu \geq \mu_n + \mu_{n-1} - 1$ we have $\operatorname{ann}_A(B_\nu) = \mathfrak{A} = \mathfrak{I}_{\mathcal{C}}$.*

Proof. Since $\mathfrak{A} = \mathfrak{I}_{\mathcal{C}}$, 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 [36, 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 6. 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 technics developed in [37, §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 $0 \leq \mu_1 \leq \cdots \leq \mu_{n-1} \leq \mu_n$). □

The following aim is to produce a matrix-based representation of $\mathcal{C}$ 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 $\mathfrak{I}_{\mathcal{C}}$. In view of Corollary 8, certain Fitting ideals associated to a μ-basis of ϕ are natural candidates for that purpose.

1.2.5 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:

$$\oplus_{i=1}^{n} C(-\mu_i) \xrightarrow{u_1,\ldots,u_n} C : (g_1, \ldots, g_n) \mapsto \sum_{i=1}^{n} u_i g_i. \tag{1.2.4}$$

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 (1.2.4), we deduce that for all $\nu \in \mathbb{N}$ the cokernel of the A-linear map

$$\oplus_{i=1}^{n} C_{\nu-\mu_i} \xrightarrow{u_1,\ldots,u_n} C_\nu : (g_1, \ldots, g_n) \mapsto \sum_{i=1}^{n} u_i g_i \tag{1.2.5}$$

is exactly the A-module B_ν. From here, a well known result of commutative algebra allows to approximate the ideal $\mathrm{ann}_A(B_\nu)$ 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 (1.2.5). Indeed, it is well known that (see for instance [33, Proposition 20.7] or [38, Theorem 5, Chapter 3])

$$\mathrm{ann}_A(B_\nu)^{\nu+1} \subset \mathfrak{F}(B_\nu) \subset \mathrm{ann}_A(B_\nu). \tag{1.2.6}$$

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

Theorem 9. *For all integer $\nu \geq \mu_n + \mu_{n-1} - 1$, we have $V(\mathfrak{F}(B_\nu)) = \mathcal{C}$.*

Proof. Straightforward from the Corollary 8 and (1.2.6). □

For all integer $\nu \geq \mu_n + \mu_{n-1} - 1$ denote by $\mathtt{M}(\phi)_\nu$ a matrix of the A-linear map (1.2.5). 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). So 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 $\mathcal{C}$.

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

Definition 10. 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 $\mathcal{C}$, 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 $\mathcal{C}$. Given an integer $\nu \geq \mu_n + \mu_{n-1} - 1$, the ideal $\mathfrak{F}(B_\nu)$ is not equal to the defining ideal $\mathfrak{I}_\mathcal{C}$ of the rational curve $\mathcal{C}$ in general (see Example 12). However, $\mathfrak{F}(B_\nu)$ is almost everywhere algebraically faithful to the parameterization ϕ in the following sense.

Theorem 11. *For all integer $\nu \geq \mu_n + \mu_{n-1} - 1$, we have the following equality of ideals in the ring $A_{\mathfrak{I}_\mathcal{C}}$ which denotes the localization of A by the prime ideal $\mathfrak{I}_\mathcal{C}$:*

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

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

Proof. Since $\mathfrak{I}_\mathcal{C} = \mathfrak{A} = \operatorname{ann}_A(B_\nu)$, 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 $(B_\nu)_\mathfrak{A} \simeq (A/\mathfrak{A}A)_\mathfrak{A}^{\deg(\phi)}$. Using classical properties of Fitting ideals (see for instance [38, §3.1]) we deduce that

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

as claimed. □

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

Notice that in the rest of this chapter, 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 12. Let $\mathcal{C}$ be the rational space curve parameterized by

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

A μ-basis of $\mathcal{C}$ is given by

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

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` [39], we get that $\mathfrak{I}_{\mathcal{C}} = (z^2 - xw, y^2 - xz)$ and that

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

This computation shows that ϕ is birational onto $\mathcal{C}$ by Theorem 11 and also that $\mathfrak{F}(B_2)$ has an embedded component supported at the point $(0 : 0 : 0 : 1) \in \mathcal{C}$. Therefore, $\mathfrak{F}(B_\nu) \neq \mathfrak{I}_{\mathcal{C}}$ (notice that the third component in the decomposition of $\mathfrak{F}(B_\nu)$ is (x, y, z, w)-primary).

1.2.6 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 $\mathcal{C}$ among the ones given in Definition 10.

1. *Compute a μ-basis as* (1.2.1) *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* (1.2.3).
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 [13].

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 [40]) 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 (1.2.5). 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 $\mathcal{C}$. 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 chapter how one can take advantage of such a representation to perform important operations of CAGD, as the curve/curve intersection problem or the detection of singular locus.

1.2.7 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 $\mathcal{C}$ is a plane curve and $\mathfrak{I}_{\mathcal{C}}$ is a principal ideal. It follows that $\mathcal{C}$ 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 $\mathcal{C}$ 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 11 contains the fact the $\det(\mathtt{M}(\phi)_{d-1})$ is equal to an implicit equation of $\mathcal{C}$ 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 $\mathcal{C}$ 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

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

so that $\mathcal{C}$ 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

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

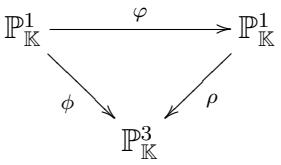
Let us end this paragraph with a last particular case: a line in $\mathbb{P}^3$ (we restrict ourselves to $\mathbb{P}^3$ for simplicity). Such a case occurs when $\mu_1 = \mu_2 = 0$. By a linear change of coordinates, we can suppose that $u_1 = x$, $u_2 = y$ and $u_3 = p(s,t)z + q(s,t)w$. Notice that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

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

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

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

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 $\mathfrak{F}(B_\nu) = {I_\mathcal{C}}^{\deg(\phi)}$ in this case. This last property follows from Luröth Theorem (see for instance [41]). Indeed, this theorem implies that there exists a commutative diagram



where

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

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

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

1.2.8 Matrix representations without μ-bases

In Section 1.2 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 [13, 42]), 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 1.2 and set

$$\Delta_{i,j} = \left|\begin{array}{cc} f_i(s,t) & f_j(s,t) \\ x_i & x_j \end{array}\right|$$

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

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

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

As in Section 1.2, set $A=\mathbb{K}[x_0,\dots,x_n]$, $C=A[s,t]$ 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

$$\bigoplus_{0\leq i<j\leq n} C(-d) \xrightarrow{(\dots,\Delta_{i,j},\dots)} C : (\cdots : g_{i,j} : \cdots) \mapsto \sum_{0\leq i<j\leq n} g_{i,j}\Delta_{i,j} \tag{1.2.7}$$

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

Proposition 13. *For all integer $\nu\geq 2d-1$, we have $B_\nu=\overline{B}_\nu$.*

Proof. Consider the Koszul complex associated to the sequence $(f_0,\dots,f_n)$ 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 $(f_0,\dots,f_n)$. 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 [37]) 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 (1.2.7), for all integer $\nu\in\mathbb{N}$ we obtain the A-linear map

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

Denote by $\overline{\mathtt{M}(\phi)}_\nu$ a matrix of this map. Then, by Proposition 13, we have

Corollary 14. *For all integer $\nu\geq 2d-1$, the matrix $\overline{\mathtt{M}(\phi)}_\nu$ is a representation matrix of $\mathcal{C}$.*

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

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

Chapter 2

Intersection problems with rational curves

In the first chapter, we introduced and studied the matrix-based implicit representations of rational curves and rational surfaces. In this chapter, we will show how to use matrix-based implicit representations of rational curves and surfaces to solve some important problems in CAGD, namely the curve/curve and curve/surface intersection problems, the point-on-curve and inversion problems, the detection of singularities.

The idea of using matrix representations in CAGD to solve the intersection problems is quite old. The novelty of our contribution is to enable *non square* matrices, extension which is motivated by recent research in this topic. We show how to manipulate these representations by proposing a dedicated algorithm to address the curve/curve and curve/surface intersection problem by means of numerical linear algebra techniques.

The point-on-curve and inversion problems, the detection of singularities have been considered recently in [13, 14, 18] with methods based on a set of equations that are built from a μ-basis of the parameterization. We will show in this chapter 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 results in this chapter have been published in two articles. The first one is a joint work with Laurent Busé and Bernard Mourrain and have been published in [43]. The second one is a joint work with Laurent Busé and have been published in [25]

Throughout this chapter, we assume that $\mathbb{K}$ is an algebraically closed field, typically the field of complex numbers $\mathbb{C}$.

2.1 Reduction of a univariate pencil of matrices

In this part, we will develop a numerical method to reduce generalized pencils of matrices. More precisely, in the theory of Kronecker forms (see for instance [44, Chapter 12]) we will reduce such a pencil to its *regular* part, avoiding this way the *non square* Kronecker blocks.

2.1.1 Linearization of a polynomial matrix

We begin with some notation.

Let A and B be two matrices of size $m \times n$. 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 $\lambda(A, B) = \lambda(AB^{-1}, I) = \lambda(AB^{-1})$, which is the ordinary spectrum of AB^{-1}. The previous definition of generalized eigenvalues extends naturally to a polynomial matrix $M(t)$, where the entries are polynomials in t of any degree.

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 16. 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

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

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

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

We have the following interesting property that follows from a straightforward computation.

Proposition 17. *With the above notation, for all $t \in \mathbb{K}$ and all vector $v \in \mathbb{K}^m$ we have*

$$M^t(t)v = 0 \Leftrightarrow (A - tB) \begin{pmatrix} v \\ tv \\ \vdots \\ t^{d-1}v \end{pmatrix} = 0.$$

Because $\operatorname{rank} M(t) = \operatorname{rank} M^t(t)$, from now on we will assume that $M(t)$ is an $m \times n$-matrix such that $m \leq n$. Therefore, $\operatorname{rank} M(t)$ drops if and only if $\operatorname{rank} M(t) < m$.

Theorem 18. *With the above assumptions, the following equivalence holds:*

$$\operatorname{rank} M(t) < m \Leftrightarrow \operatorname{rank}(A - tB) < dm.$$

Proof. Because $\operatorname{rank} M(t) = \operatorname{rank} M^t(t)$, we have that $\operatorname{rank} M^t(t) < m$. Thus, there exists a column vector $v \neq 0$ such that $M^t(t)v = 0$. Then, by Proposition 17 equation $(A - tB)x = 0$ has a nonzero root. That means exactly that $\operatorname{rank}(A - tB) < dm$.

Now, if $\operatorname{rank}(A - tB) < dm$, then equation $(A - tB)x = 0$ have a root $x \neq 0$ and by a straightforward computation it is of the form

$$x = \begin{pmatrix} v \\ tv \\ \vdots \\ t^{d-1}v \end{pmatrix}.$$

Since $x \neq 0$ and by Proposition 17, we have $v \neq 0$ and v is a root of equation $M^t(t)v = 0$. Thus, $\operatorname{rank} M^t(t) < m$ and it follows that $\operatorname{rank} M(t) < m$. □

By Theorem 18, we transformed the computation of generalized eigenvalues of the matrix polynomial $M(t)$ (that is to say the roots of the gcd of the maximal minors of $M(t)$) into the computation of generalized eigenvalues of a pencil of matrices $A - tB$. If the matrices A, B were two square matrices, then we could easily compute their generalized eigenvalues by the QZ-algorithm [45]. Therefore, our next task is to reduce the pencil $A - tB$ into a square pencil that keeps the information we are interested in.

Before moving on, we recall what is the Smith form of $M(t)$ for future use. Assume that $\operatorname{rank} M(t) = r$, it exists two regular polynomial matrices with nonzero determinant in $\mathbb{K}$, say $P(t)$ and $Q(t)$, such that

$$D(t) \quad = \quad P(t)M(t)Q(t) \quad = \quad \begin{pmatrix} a_r(t) & 0 & \dots & \dots & \dots & 0 \\ 0 & a_{r-1}(t) & 0 & \dots & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & \dots & a_1(t) & \dots & 0 \\ 0 & 0 & \dots & \dots & \dots & 0 \end{pmatrix}$$

where $a_i(t)$'s are monic polynomials and $a_i(t)$ divides $a_{i-1}(t)$. This form is unique and is called the Smith form of $M(t)$ (see for instance [46, Chapter 6]). Notice that by performing unimodular row and column transformations on the matrix $A - tB$, we can find that $A - tB$ has the Smith form (see for instance [47,48] for more details)

$$U(t)(A - tB)V(t) = \text{diag}\{I_m, ..., I_m, D(t)\}$$

where $D(t)$ is the Smith form of $M^t(t)$. Thus, Theorem 18 can be recovered from this property.

2.1.2 The Kronecker form of a non square pencil of matrices

Hereafter, we recall some known properties of the Kronecker form of pencils of matrices.

Definition 19. Let $L_k(t), \Omega_k(t)$ be the two matrices of size $k \times (k+1)$ and $k \times k$ respectively, defined by

$$L_k(t) = \begin{pmatrix} 1 & t & 0 & \dots & 0 \\ 0 & 1 & t & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & 1 & t & 0 \\ 0 & 0 & \dots & 1 & t \end{pmatrix},$$

$$\Omega_k(t) = \begin{pmatrix} 1 & t & 0 & \dots & 0 \\ 0 & 1 & t & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & \dots & 1 & t \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix}.$$

We are going to use the following theorem, which gives what is called the Kronecker canonical form of a pencil of matrices (see for instance [44, p. 31-34]).

Theorem 20. *For any couple constant matrices A, B of size $p \times q$, there exist constant invertible matrices P and Q such that the pencil $P(A - tB)Q$ is of the block-diagonal form*

$$diag\{L_{i_1}, ..., L_{i_s}, L^t_{j_1}, ..., L^t_{j_u}, \Omega_{k_1}, ..., \Omega_{k_v}, A' - tB'\}$$

where A', B' are square matrices and B' is invertible. The dimension $i_1, ..., i_s, j_1, ..., j_u, k_1, .., k_v$ and the determinant of $A' - tB'$ (up to a scalar) are independent of the representation.

This theorem can be implemented as follows:

Proposition 21. *For any couple of matrices C_0, C_1 of size $p \times q$, there exist unitary matrices U and V such that the pencil*

$$U(C_0 - tC_1)V = \tilde{C}_0 - t\tilde{C}_1$$

is of the form

$$\tilde{C}(t) = \begin{pmatrix} \tilde{C}_l(t) & \tilde{C}_{1,2}(t) & \tilde{C}_{1,3}(t) \\ 0 & \tilde{C}_r(t) & \tilde{C}_{2,2}(t) \\ 0 & 0 & \tilde{C}_{reg}(t) \end{pmatrix}$$

where

- *$\tilde{C}_l(t) = \tilde{C}_{l,0} - t\tilde{C}_{l,1}$ has only blocks of the form $L_k(t), \Omega_k(t)$ in its Kronecker canonical form,*
- *$\tilde{C}_r(t) = \tilde{C}_{r,0} - t\tilde{C}_{r,1}$ has only blocks of the form $L^t_k(t)$,*
- *$\tilde{C}_{reg}(t) = \tilde{C}_{reg,0} - t\tilde{C}_{reg,1}$ is a square regular pencil.*

It is interesting to notice that the above decomposition can be computed within $O(p^2q)$ arithmetic operations. We refer the reader to [49, 50] for a proof, as well as for an analysis of the stability of this decomposition.

Following the ideas developed in [49,50] and the reduction methods exploited in [51,52], we now describe an algorithm that allows to remove the Kronecker blocks L_k, L_k^t and Ω_k of the pencil of matrices $A - tB$ in order to extract the regular pencil $A' - tB'$.

2.1.3 The Algorithm for 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 $p\times q$. Set $\rho = \operatorname{rank} B$. In the following algorithm, all computational steps are easily realized via the classical LU-decomposition.
Remark that a matrix is in column echelon form if it is written under the form

$$\begin{pmatrix} * & * & * & \dots & \dots & * \\ * & * & * & \dots & \dots & * \\ * & \dots & \dots & * & 0 & 0 \\ * & * & \dots & * & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ * & * & 0 & 0 & 0 & 0 \end{pmatrix}$$

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

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

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

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

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

$$P_1 A_{1,2} Q_1 = \left(\begin{array}{c} A'_{1,2} \\ \hline 0 \end{array}\right)$$

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

$$P_1 A_1 Q'_1 = \left(\begin{array}{c|c} A'_{1,1} & A'_{1,2} \\ \hline A_2 & 0 \end{array}\right) \quad P_1 B_1 Q'_1 = \left(\begin{array}{c|c} B'_{1,1} & 0 \\ \hline B_2 & 0 \end{array}\right)$$

where

- $Q'_1 = \left(\begin{array}{c|c} I_\rho & 0 \\ \hline 0 & Q_1 \end{array}\right)$, I_ρ is the identity matrix of size ρ.

- $A'_{1,2}$ 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 $\operatorname{rank} B_j = q_j$.

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.

2.2 Curve/surface intersection

Suppose given an algebraic surface $\mathbf{S}$ represented by a homogeneous and irreducible implicit equation $S(x, y, z, w) = 0$ in $\mathbb{P}^3_{\mathbb{K}}$ and a rational space curve $\mathbf{C}$ represented by a parameterization

$$\Psi : \mathbb{P}^1_{\mathbb{K}} \to \mathbb{P}^3_{\mathbb{K}} : (s : t) \mapsto (x(s,t) : y(s,t) : z(s,t) : w(s,t))$$

where $x(s,t), y(s,t), z(s,t), w(s,t)$ are homogeneous polynomials of the same degree and without common factor in $\mathbb{K}[s,t]$.

A standard problem in non linear computational geometry is to determine the set $\mathbf{C} \cap \mathbf{S} \subset \mathbb{P}^3_{\mathbb{K}}$, especially when it is finite. One way to proceed, is to compute the roots of the homogeneous polynomial

$$S(x(s,t), y(s,t), z(s,t), w(s,t)) \tag{2.2.1}$$

because they are in correspondence with $\mathbf{C} \cap \mathbf{S}$ through the regular map Ψ. Observe that (2.2.1) is identically zero if and only if $\mathbf{C} \cap \mathbf{S}$ is infinite, equivalently $\mathbf{C} \subset \mathbf{S}$ (for $\mathbf{C}$ is irreducible).

If $\mathbf{S}$ is a rational surface represented by a parameterization, then several authors (see for instance [8] and the references therein) used some *square* matrix representations, most of the time obtained from a particular resultant matrix, of $\mathbf{S}$ in order to compute the set $\mathbf{C} \cap \mathbf{S}$ by means of eigencomputations. As we have already mentioned, such square matrix representations exist only under some restrictive conditions. Hereafter, we would like to generalize this approach for non square matrix representation that can be obtained for a much larger class of rational surfaces and are very easy to compute.

So, assume that $M(x, y, z, w)$ is a matrix representation of the surface $\mathbf{S}$, meaning a representation of the polynomial $S(x, y, z, w)$. By replacing the variables x, y, z, w by the homogeneous polynomials $x(s,t), y(s,t), z(s,t), w(s,t)$ respectively, we get the matrix

$$M(s,t) = M(x(s,t), y(s,t), z(s,t), w(s,t))$$

and we have the following easy property:

Lemma 22. *With the above notation, for all point* $(s_0 : t_0) \in \mathbb{P}^1_{\mathbb{K}}$ *the rank of the matrix* $M(s_0, t_0)$ *drops if and only if the point* $(x(s_0, t_0) : y(s_0, t_0) : z(s_0, t_0) : w(s_0, t_0))$ *belongs to the intersection locus* $\mathbf{C} \cap \mathbf{S}$.

It follows that points in $\mathbf{C} \cap \mathbf{S}$ associated to points $(s : t)$ such that $s \neq 0$, are in correspondence with the set of values $t \in \mathbb{K}$ such that $M(1, t)$ drops of rank strictly less than its row and column dimensions i.e. the set of generalized eigenvalues of $M(1, t)$.

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

Algorithm 2: Matrix intersection algorithm

Input: A matrix representation of a surface $\mathbf{S}$ and a parametrization of a rational space curve $\mathbf{C}$.

Output: The intersection points of $\mathbf{S}$ and $\mathbf{C}$.

1. Compute the matrix representation M(t).

2. Compute the generalized companion matrices A and B of M(t).

3. Compute the companion regular matrices A' *and* B'.

4. Compute the eigenvalues of (A', B').

5. For each eigenvalue t_0*, the point* $P(x(t_0) : y(t_0) : z(t_0) : w(t_0))$ *is one of the intersection points.*

2.2.1 The multiplicity of an intersection point

In this section, we analyze more precisely the multiplicity of an intersection point and show its correlation with the corresponding eigenvalue multiplicity for the polynomial matrix $M(1, t)$. We assume hereafter, without loss of generality, that the intersection point is at finite distance.

Let $(\Delta_i(x, y, z, w))_{i=1,\ldots,N}$ be the set of all maximal minors of a representation matrix $M(x, y, z, w)$ of $\mathbf{S}$. By definition, for all $i = 1, \ldots, N$ there exists a polynomial $H_i(x, y, z, w)$ such that $\Delta_i = H_i S$ and $\gcd(H_1, \ldots, H_N)$ is a nonzero constant in $\mathbb{K}[x, y, z, w]$. Therefore, the zero locus of the polynomials $H_1, \ldots, H_N, S$ is an algebraic variety $\mathbf{W}$ which is included in $\mathbf{S}$ and which has projective dimension at most one.

Hereafter, we will often abbreviate $x(1, t)$ by $x(t)$ to not overload the text, and will do similarly for the other polynomials y, z, w. Let $P = (x(t_0) : y(t_0) : z(t_0) : w(t_0))$ be a point on the parameterized curve $\mathbf{C}$. The intersection multiplicity of $\mathbf{S}$ and $\mathbf{C}$ at P can be defined as

$$I_P = \sum_{t_i \text{ such that } \Psi(t_i)=P} \dim_{\mathbb{K}} \left(\frac{\mathbb{K}[t]}{S(x(t), y(t), z(t), w(t))} \right)_{(t-t_i)}$$

assuming w.l.o.g. that Ψ is birational onto $\mathbf{C}$ (by Lurőth Theorem [41]) and that all the preimages of P are at finite distance (that can be achieved by a linear change of coordinates).

Of course, if $P \in \mathbf{C} \cap \mathbf{S}$ then $I_P > 0$ and $I_P = 0$ otherwise. Also, if P is non singular point on $\mathbf{C}$ (recall that the set of singular points on $\mathbf{C}$ is finite) then

$$I_P = \dim_{\mathbb{K}} \left(\frac{\mathbb{K}[t]}{S(x(t), y(t), z(t), w(t))} \right)_{(t-t_0)}$$

Now, denote by m_λ the multiplicity of λ as a generalized eigenvalue of the matrix $M(t) = M(x(t), \ldots, w(t))$. From the above considerations, it follows that the intersection multiplicity of a point $P = (x(t_0) : y(t_0) : z(t_0) : w(t_0)) \in \mathbf{C} \cap \mathbf{S}$ such that $P \notin \mathbf{W}$ is exactly the sum of the multiplicity of the corresponding eigenvalues:

$$I_P = \sum_{t_i \text{ such that } \Psi(t_i)=P} m_{t_i}$$

As already noticed, if P is moreover smooth on $\mathbf{C}$, then $I_P = m_{t_0}$. Now, if $P \in \mathbf{W} \cap \mathbf{C} \cap \mathbf{S}$, then

$$I_P < \sum_{t_i \text{ such that } \Psi(t_i)=P} m_{t_i}$$

due to the existence of embedded components (determined by the polynomials H_i's) that come from the matrix representation of $\mathbf{S}$.

Notice that if the surface $\mathbf{S}$ is given by a parameterization which is not birational onto its image, then the matrix representations that we describe in the first chapter actually represent the implicit equation of $\mathbf{S}$ up to a certain power, say β. In such case, one has similar results regarding the multiplicities of intersection points:

$$\beta I_P = \sum_{t_i \text{ such that } \Psi(t_i)=P} m_{t_i}$$

If P is smooth on $\mathbf{C}$, then $\beta I_P = m_{t_0}$ and

$$\beta I_P < \sum_{t_i \text{ such that } \Psi(t_i)=P} m_{t_i}$$

if $P \in \mathbf{W} \cap \mathbf{C} \cap \mathbf{S}$.

Now, we are going to relate this multiplicity with the multiplicity of the corresponding eigenvalue of the pencil of matrices built in Section 2.1.3.

With the notations of Section 2.1.3, we have:

Proposition 23. *We have*

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

Proof. It follows from the fact that the Kronecker blocks $L_{i_1}, ..., L_{i_s}, L^t_{j_1}, ..., L^t_{j_u}, \Omega_{k_1}, ..., \Omega_{k_v}$ have all full rank. □

Assume that matrix $M^t(t)$ has the Smith form

$$\begin{pmatrix} a_r(t) & 0 & \ldots & \ldots & \ldots & 0 \\ 0 & a_{r-1}(t) & 0 & \ldots & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \ldots & \ldots & a_1(t) & \ldots & 0 \\ 0 & 0 & \ldots & \ldots & \ldots & 0 \end{pmatrix}$$

We set

$$U(t) = \begin{pmatrix} a_s(t) & 0 & \dots & \dots & 0 \\ 0 & a_{s-1}(t) & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & \dots & 0 & a_1(t) \end{pmatrix}$$

Notice that $U(t)$ is a square matrix where $a_1(t), \dots, a_s(t)$ are monic non constant polynomials.

Proposition 24. *The Smith form of the regular pencil $A' - tB'$ is of the form $\{I_k, U(t)\}$.*

Proof. We know that the matrix $A - tB$ has the Kronecker form

$$\text{diag}\{L_{i_1}, ..., L_{i_s}, L^t_{j_1}, ..., L^t_{j_u}, \Omega_{k_1}, ..., \Omega_{k_v}, A' - tB'\}$$

and the Smith form (see for instance [47])

$$\text{diag}\{I_m, ..., I_m, D(t)\}.$$

On the other hand, we easily see that the Kronecker blocks $L_k(t), L^t_k(t)$ and $\Omega_k(t)$ have respectively the Smith form

$$\begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & 1 & 0 & 0 \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & \dots & 0 & 1 \\ 0 & 0 & \dots & 0 & 0 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & \dots & 1 & 0 \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix}.$$

Therefore, the regular pencil $A' - tB'$ has the Smith form $\{I_k, U(t)\}$. □

Theorem 25. *If $A' - tB'$ denotes the regular part of a pencil associated to a representation matrix of the intersection between a surface $\mathbf{S}$ and a rational parametric curve $\mathbf{C}$ then the intersection multiplicity of $\mathbf{S}$ and $\mathbf{C}$ at a point $P = (x(t_0) : y(t_0) : z(t_0) : w(t_0))$ is equal to the multiplicity of the eigenvalues (A', B') at t_0, except in few cases where this multiplicity is strictly bigger.*

Proof. Because $M(t)$ is the $m \times n$-matrix ($m \leq n$) representation of the intersection between $\mathbf{S}$ and $\mathbf{C}$, $M^t(t)$ has the Smith form

$$\begin{pmatrix} a_m(t) & 0 & \dots & \dots & \dots & 0 \\ 0 & a_{m-1}(t) & 0 & \dots & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & \dots & \dots & \dots & a_1(t) \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & \dots & \dots & 0 \end{pmatrix},$$

Let $F(t) = a_m(t)a_{m-1}(t)...a_1(t)$. By Proposition 24, we have $F(t) = c\det(A' - tB')$, where c is a nonzero constant.The multiplicity of the eigenvalue of (A', B') at t_0 is equal to the multiplicity of the root t_0 of $F(t)$ and therefore to the multiplicity of $\mathbf{S}$ and $\mathbf{C}$ at a point $P = (x(t_0) : y(t_0) : z(t_0) : w(t_0))$, expect in few cases that are described in Section 2.2.1. □

Remark 26. In the statement of this theorem, the few cases where the multiplicity as an intersection point is strictly less than the multiplicity of the corresponding generalized eigenvalue are exactly the cases where the curve cut out the surface on $\mathbf{W}$, taking again notation of Section 2.2.1. It turns out that $\mathbf{W}$ is a closed variety in $\mathbf{S}$ and hence the measure of $\mathbf{W}$ in $\mathbf{S}$ is null. Therefore, these cases have a null probability to happen if the surface and the curve are supposed arbitrary.

We have implemented our curve/surface intersection algorithm, as well as the matrix representations given in the first chapter, in the software MAPLE or the software MATHEMAGIX. Hereafter, we provide some examples to illustrate it.

Example 27. Let $\mathbf{S}$ be the rational surface which is parametrized by

$$\phi : \mathbb{P}^2 \to \mathbb{P}^3 : (s : t : u) \mapsto (f_1 : f_2 : f_3 : f_4)$$

where

$$f_1 = s^3 + t^2u, f_2 = s^2t + t^2u, f_3 = s^3 + t^3, f_4 = s^2u + t^2u.$$

We want to compute the intersection of $\mathbf{S}$ and the rational curve $\mathbf{C}$, often called the twisted cubic, given by the parameterization

$$x(t) = 1, y(t) = t, z(t) = t^2, w(t) = t^3.$$

First, on computes a matrix representation of $\mathbf{S}$:

$$\begin{pmatrix} 0 & 0 & 0 & w-y & 0 & 0 & z-x \\ w & 0 & 0 & x & w-y & 0 & 0 \\ x-y-z & 0 & 0 & -z & 0 & w-y & 0 \\ 0 & w & 0 & 0 & x & 0 & -y \\ 0 & x-y-z & w & 0 & -z & x & y+z-x \\ 0 & 0 & x-y-z & 0 & 0 & -z & 0 \end{pmatrix}$$

A point P at finite distance belongs to the intersection locus of $\mathbf{S}$ and $\mathbf{C}$ if and only if $P = (1 : t : t^2 : t^3)$ and t is one of the generalized eigenvalues of the following matrix $M(t)$ given by

$$\begin{pmatrix} 0 & 0 & 0 & t^3-t & 0 & 0 & t^2-1 \\ t^3 & 0 & 0 & 1 & t^3-t & 0 & 0 \\ 1-t-t^2 & 0 & 0 & -t^2 & 0 & t^3-t & 0 \\ 0 & t^3 & 0 & 0 & 1 & 0 & -t \\ 0 & 1-t-t^2 & -t^3 & 0 & -t^2 & 1 & t^2+t-1 \\ 0 & 0 & 1-t-t^2 & 0 & 0 & -t^2 & 0 \end{pmatrix}$$

We have $M(t) = M_3t^3 + M_2t^2 + M_1t + M_0$ where M_0, M_1, M_2, M_3 are respectively

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$\begin{pmatrix} 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & -1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & -1 & 0 & 1 \\ 0 & 0 & -1 & 0 & 0 & -1 & 0 \end{pmatrix},$$

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

and the generalized companion matrices of $M(t)$ are

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

Now, applying the algorithm given in Section 2.1.3, we find that the regular part of the pencil $A - tB$ is the pencil $A' - tB'$ where A' is given by

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & -1 \\ 0 & 2 & 0 & 0 & 2 & 0 & 2 & 0 & -1 & -1 & -2 & -2 & 1 \\ 0 & -1 & 0 & 0 & -1 & 0 & -1 & 0 & 2 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & -1 & -1 & -1 & -1 & 0 \\ 0 & 1 & 0 & -1 & 1 & 0 & 1 & 0 & 0 & 0 & -1 & -1 & 1 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & -1 & -1 & 0 \\ 0 & 1 & -1 & 0 & 1 & 0 & 1 & 0 & -1 & -1 & -1 & -1 & 0 \\ 0 & -1 & 0 & 0 & -2 & 0 & -1 & 0 & 0 & 0 & 1 & 2 & -1 \end{pmatrix},$$

and B' is the identity matrix. Then, we compute the following eigenvalues: $t_1 = 1$ with multiplicity 3, $t_2 = -1$ with multiplicity 3 and the roots of the equation $Z^7 + 3Z^6 - Z^5 - Z^3 + Z^2 - 2Z + 1 = 0$.

Example 28. Let $\mathbf{S}$ be the sphere that we suppose given as the image of the parametrization

$$\phi : \mathbb{P}^2 \to \mathbb{P}^3 : (s : t : u) \mapsto (f_1 : f_2 : f_3 : f_4)$$

where

$$f_1 = s^2 + t^2 + u^2, f_2 = 2su, f_3 = 2st, f_4 = s^2 - t^2 - u^2$$

Let $\mathbf{C}$ be the twisted cubic which is parametrized by

$$x(t) = 1, y(t) = t, z(t) = t^2, w(t) = t^3.$$

The computation of a matrix representation of the sphere $\mathbf{S}$ gives

$$\begin{pmatrix} -y & 0 & z & x+w \\ 0 & -y & -x+w & -z \\ z & x+w & y & 0 \end{pmatrix}.$$

Now, a point P belongs to the intersection of $\mathbf{S}$ and $\mathbf{C}$ if and only if $P = (1 : t : t^2 : t^3)$ and t is one of the generalized eigenvalues of the matrix

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

As before, we easily compute the eigenvalues and find:

$$t_1 = 0.7373527056, t_2 = -0.7373527056,$$
$$t_3 = 0.5405361044 + 1.031515287i, t_4 = -0.5405361044 - 1.031515287i,$$
$$t_5 = 0.5405361044 - 1.031515287i, t_6 = -0.5405361044 + 1.031515287i.$$

All these eigenvalues have multiplicity 1. They all correspond to one intersection point between $\mathbf{S}$ and $\mathbf{C}$ which has multiplicity 1. By Bezout Theorem, we find here all the intersection points between these two algebraic varieties (all of them are at finite distance).

Example 29. As the previous example, let $\mathbf{S}$ be the sphere given be the same parametrization and matrix representation. Here, we want to intersect $\mathbf{S}$ with a simple curve $\mathbf{C}$: the line parametrized by

$$x(t) = 1, y(t) = 0, z(t) = 0, w(t) = t.$$

In this case we have

$$M(t) = \begin{pmatrix} 0 & 0 & 0 & t+1 \\ 0 & 0 & -1+t & 0 \\ 0 & 1+t & 0 & 0 \end{pmatrix}.$$

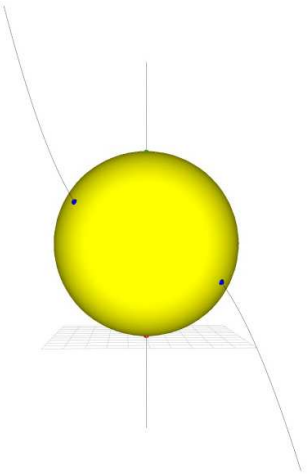


Figure 2.1: Intersection of the sphere and the twisted cubic, the axis Oz

We proceed as in the previous example and now find two eigenvalues: $t_1 = -1$ with multiplicity 2 and $t_2 = +1$ with multiplicity 1. They correspond to the intersection points $P_1(1:0:0:-1)$ and $P_2(1:0:0:1)$ respectively.

It is interesting to notice that in this case the multiplicity of the eigenvalue t_1, which is 2, is not equal to the multiplicity of the intersection point P_1, which is 1. This is due to the fact that the matrix representation of S introduces an embedded point, namely P_1 itself, on the sphere. Indeed, the four maximal minors of the matrix representation of $\mathbf{S}$ are given by

$$-y(-y^2+x^2-w^2-z^2), z(-y^2+x^2-w^2-z^2),$$
$$(x+w)(-y^2+x^2-w^2-z^2), 0.$$

Therefore, the zero locus defined by the equations $x+w$, y, z, $-y^2+x^2-w^2-z^2$, which is nothing but the point P_1, is an embedded component on the sphere.

2.3 Curve/curve intersection

Suppose given two rational curves, say $\mathcal{C}_1$ parameterized by

$$\mathbb{P}^1 \xrightarrow{\phi_1} \mathbb{P}^n : (s:t) \mapsto (f_0 : \cdots : f_n)(s,t) \tag{2.3.1}$$

and $\mathcal{C}_2$ parameterized by the regular map

$$\mathbb{P}^1 \xrightarrow{\phi_2} \mathbb{P}^n : (s:t) \mapsto (g_0 : \cdots : g_n)(s,t). \tag{2.3.2}$$

Let $\mathtt{M}(\phi)_\nu(\phi_1)$ be a representation matrix of $\mathcal{C}_1$ for a suitable integer ν, as described in Section 1.2. The substitution in $\mathtt{M}(\phi)_\nu(\phi_1)$ of the variables x, y, z, w by the homogeneous parameterization of $\mathcal{C}_2$ yields the matrix

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

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

Lemma 30. *Let* $(s_0 : t_0) \in \mathbb{P}^1$*, then* $\operatorname{rank} \mathtt{M}(\phi)_\nu(\phi_1)(s_0, t_0) < \nu + 1$ *if and only if the point* $\phi_2(s_0, t_0)$ *belongs to the intersection locus* $\mathcal{C}_1 \cap \mathcal{C}_2$*.*

The set $\mathcal{C}_1 \cap \mathcal{C}_2$ is in correspondence with the points of $\mathbb{P}^1$ where the rank of $\mathtt{M}(\phi)_\nu(\phi_1)(s,t)$ drops. By setting $t = 1$, the determination of the values of s such that the rank of $\mathtt{M}(\phi)_\nu(\phi_1)(s,1)$ 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 technics and generalized eigenvalues computations which have been extended for non-square matrices in 2.2. We are now ready to state our algorithm for solving the curve/curve intersection problem and give an illustrative example.

Algorithm 3: Intersection of two parameterized curves

Input: Two parameterized curves $\mathcal{C}_1$ and $\mathcal{C}_2$ given by (2.3.1) and (2.3.2).
Output: The intersection points of $\mathcal{C}_1$ and $\mathcal{C}_2$.
1. *Compute the matrix representation* $\mathtt{M}(\phi)_\nu(\phi_1)$ *of* $\mathcal{C}_1$ *for a suitable* ν*.*
2. *Compute the generalized companion matrices A and B of* $\mathtt{M}(\phi)_\nu(\phi_1)$*.*
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.*

Remark 31. This algorithm returns all the points in $\mathcal{C}_1 \cap \mathcal{C}_2$ except possibly the point $\phi(1:0)$. This latter point can be treated independently.

Example 32. Let $\mathcal{C}_1$ 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 $\mathcal{C}_1$ with the twisted cubic $\mathcal{C}_2$ 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 $\mathcal{C}_1$:

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

A point P at finite distance belongs to the intersection locus of $\mathcal{C}_1$ and $\mathcal{C}_2$ if and only if $P = (1 : t : t^2 : t^3)$ and t is one of the generalized eigenvalues of the matrix

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

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 3, 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 $\mathcal{C}_1$ intersect $\mathcal{C}_2$ 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 $\mathcal{C}_1$. For that purpose, we first evaluate the rank of the matrix $\mathtt{M}(\phi)_3(P)$. 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 2.3.2, but rather the method for computing the singular points of $\mathcal{C}_1$ given in Section 2.4. 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.

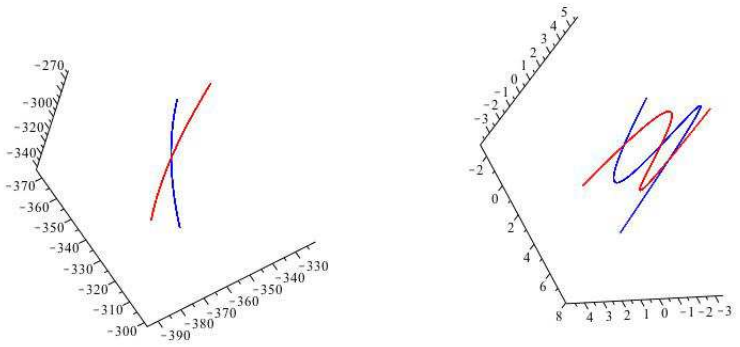
Example 33. We have implemented Algorithm 3 in the software `Maple`. The corresponding files are available at `http://www-sop.inria.fr/members/Luu.Ba_Thang/`. Consider the two curves parameterized, in affine coordinate, by

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

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 $(1, 1, 0), (0, 2, 1), (0, 3, 1)$ and $(-308, -341, -363)$ can be visualized in the following pictures.



2.3.1 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 technics 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 [19] and [20] 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

$$\begin{array}{rcl} \Phi_{\mathbb{S}} : \mathbb{P}^1_{\mathbb{K}} \times \mathbb{P}^1_{\mathbb{K}} & \rightarrow & \mathbb{P}^3_{\mathbb{K}} \\ (s:\bar{s}) \times (t:\bar{t}) & \mapsto & (f_0(s,\bar{s},t,\bar{t}) : \cdots : f_3(s,\bar{s},t,\bar{t})) \end{array} \tag{2.3.3}$$

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

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

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 $\mathfrak{S} \subset \mathbb{P}^5$. For more detail, see [34, Lecture 6].

Plücker curves Now, returning to the ruled surface (2.3.3), 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 4: 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 $\mathcal{C}_1$ and $\mathcal{C}_2$ associated to the ruled surfaces $\mathbb{S}_1$ and $\mathbb{S}_2$ respectively.
2. Compute the intersection points of $\mathcal{C}_1$ and $\mathcal{C}_2$ using Algorithm 3.
3. Each intersection point is obtained as a value $(s : \bar{s}) \in \mathbb{P}^1$ that corresponds to the intersection line $L^{\mathbb{S}_1}_{(s:\bar{s})}$.

2.3.2 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 [13], and also by describing the curve $\mathcal{C}$ as the intersection of three

surfaces in [14], 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 $\mathcal{C}$ 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

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

This property answers the point-on curve problem.

Example 34. 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 $\mathcal{C}$ 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 $\mathcal{C}$ 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 $\mathcal{C}$.

This example is taken from [14, Example 3.7]. There, the authors' approach is to represent the curve $\mathcal{C}$ as the intersection of three surfaces, namely

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

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

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

It turns out that P belongs to the intersection of these three surfaces, but not to the curve $\mathcal{C}$. 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, correct this default.

Another classical problem is the inversion problem. In [13] 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

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

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

Example 35. Take again Example 34. 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 $\mathcal{C}$. 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 $P = \phi(1:1)$.

2.4 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 [18], 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 1.2 of the first chapter . It can be seen as an extension of what is called *singular factors* for the case of rational plane curves in [53]; see also [54]. Remark that the computation of the singular points have been detected in [55] via the generalized resultant method.

2.4.1 Rank of a representation matrix at a singular point

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

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

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 $\mathcal{C}$. 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 $\mathcal{C}$ 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 $\mathbb{K}[s,t]$

$$H(f_0(s,t), f_1(s,t), f_2(s,t), f_3(s,t)) = \prod_{i=1}^{d} (t_i s - s_i t) \tag{2.4.1}$$

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 $\mathcal{C}$ with $\mathcal{H}$ at the point P, denoted $i_P(\mathcal{C}, \mathcal{H})$, as the number of points $(s_i : t_i)_{i=1,\ldots,d}$ such that $\phi(s_i : t_i) = P$.

Definition 36. The multiplicity $m_P(\mathcal{C})$ of the point P on $\mathcal{C}$ is defined as the minimum of the intersection multiplicity $i_P(\mathcal{C}, \mathcal{H})$ where $\mathcal{H}$ runs over all the hyperplanes not containing $\mathcal{C}$ and passing through the point $P \in \mathcal{C}$, minimum which is reached with a sufficiently generic such $\mathcal{H}$.

Definition 37. An *inversion formula* of the point P on $\mathcal{C}$ is a homogeneous polynomial $h_P(s,t) \in \mathbb{K}[s,t]$ of degree $m_p(\mathcal{C})$ such that h_P divides (2.4.1) 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 [18] (we provide here a short proof for the sake of completeness).

Lemma 38. *Let P be a point on $\mathcal{C}$. 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 1.2, for all integer $\nu \geq m + n - 1$ we have a representation matrix $\mathtt{M}(\phi)_\nu$ of the curve $\mathcal{C}$ 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 39. *Given a point P in $\mathbb{P}^3$, for all integer $\nu \geq m + n - 1$ we have*

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

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

Proof. From Lemma 38, 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 $m_P(\mathcal{C})$. From Section 1.2, 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 $\nu \geq m + n - 2m_P(\mathcal{C}) - 1$. But then, multiplying this equality by the homogeneous polynomial h_P we obtain

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

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

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

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

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

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

Moreover, an immediate consequence of this theorem and Lemma 38 is that if P is a singular point on $\mathcal{C}$ then necessarily

$$2 \leq m_P(\mathcal{C}) \leq n \text{ or } m_P(\mathcal{C}) = m. \tag{2.4.2}$$

We refer the reader to [18] for more results of this kind about the possible singularities on $\mathcal{C}$ with respect to the μ-basis of its parameterization.

2.4.2 Singular factors

Theorem 39 suggests to introduce the *singular factors* of a representation, similarly to what has been done in [53], then in [54], for the case of plane curves. Although we are not able to get results similar to those proved in [54] 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 $\mathcal{C}$ 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 40. 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 41. *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 $P \in \mathcal{C}$, the inversion formula $h_P(s,t)$ divides $d_{m_P(\mathcal{C})}(s,t)$ and is coprime with $d_k(s,t)$ for all $k > m_P(\mathcal{C})$.*

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 38 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 $k = 1, \ldots, \nu+1-m_P(\mathcal{C})$ which implies that $h_P(s,t)$ and $d_k(s,t)$ are relatively prime polynomials for all $k > m_P(\mathcal{C})$. On the other hand, $P \in V(I_{\nu+1-m_P(\mathcal{C})+1}(\mathtt{M}(\phi)_\nu))$, that is $I_{\nu+1-m_P(\mathcal{C})+1}(\mathtt{M}(\phi)_\nu) \subset (x_0, x_1, x_2)$, and hence

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

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

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

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

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

Corollary 42. *Let $P = \phi(s_0 : t_0)$ be a point on $\mathcal{C}$, then $d_{m_P(\mathcal{C})}(s_0 : t_0) = 0$ and $d_k(s_0 : t_0) \neq 0$ for all $k > m_P(\mathcal{C})$. In particular, the multiplicity of P is the highest integer k such that $d_k(s_0 : t_0) = 0$.*

Corollary 43. *For any integer k such that $2 \leq k \leq m$, the product*

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

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

2.4.3 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 $\mathcal{C}$ 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 u 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 38.

We conclude this section with two illustrative examples.

Example 44 ([18, Example 7.6])**.** Let $\mathcal{C}$ 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 $\mathcal{C}$ is given by

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

From $\deg(q) = \deg(r) = 2$, we can choose $\nu = 3$, then a matrix representation of $\mathcal{C}$ 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 $\mathcal{C}$ are $d_4(s,t) = 1, d_3(s,t) = 1, d_2(s,t) = s^2t^2$. Thus, $\mathcal{C}$ 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 45. Let $\mathcal{C}$ 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 $\mathcal{C}$ 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 $\mathcal{C}$ 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 $\mathcal{C}$ are $d_3(s,t) = 1, d_2(s,t) = 1$: we recover the well known fact that $\mathcal{C}$ has no singular point.

Chapter 3

The rational surface/surface intersection problems

In the first and second chapters, we introduced and studied the matrix-based implicit representation of rational surfaces and showed how to use them to compute curve/curve and curve/surface intersection loci. In this chapter, we extend the approach developed in the second chapter for decomposing the parameterized surface/surface intersection locus. Unlike the case of solving the curve/curve and curve/surface intersection problems, addressing the surface/surface intersection problem by means of matrix representation is much more complicated because it requires to compute generalized eigenvalues of bivariate pencils of matrices.

Following the approach that we used in the second chapter, to solve the surface/surface intersection problem we will develop an algorithm that consists in two main steps. The first one is the computation of a matrix representation of one of the surface from its parameterization. After mixing this matrix representation with the parameterization of the other surface, the second step consists in a reduction of a bivariate pencil of matrices and the computation of its continuous and discrete spectrums, via the $\Delta W - 1$ decomposition algorithm that has been introduced by Kublanovskaya in [22].

Throughout this chapter, we assume that $\mathbb{C}$ is the field of complex numbers.

3.1 Reduction of a bivariate pencil of matrices

3.1.1 Linearization of a two parameter polynomial matrices

Let $M(s,t)$ be a matrix of size $m \times n$ depending on the two variables s and t. The spectrum of $M(s,t)$ is defined to be the set

$$\{(s_0,t_0) \in \mathbb{C} \times \mathbb{C} : \operatorname{rank}(M(s_0,t_0))\} < \rho$$

where $\rho := \operatorname{rank} M(s,t)$. Denote by $M_{i_1,...,i_\rho}^{j_1,...,j_\rho}$ the matrix obtained from $M(s,t)$ by taken ρ rows $i_1,...,i_\rho$ and ρ columns $j_1,...,j_\rho$, $1 \leq i_1 < ... < i_\rho \leq m$, $1 \leq j_1 < ... < j_\rho \leq n$. The coordinates of its spectrum are the common roots of all the algebraic equations

$$\det M_{i_1,...,i_\rho}^{j_1,...,j_\rho} = 0 \tag{3.1.1}$$

The one-dimensional and zero-dimensional roots of the system (3.1.1) determine respectively the one-dimensional and zero-dimensional eigenvalues of the matrix $M(s,t)$. We recall that the one dimensional eigenvalues (also called eigencurves) form the continuous part of the spectrum which is defined by the equation $\phi(s,t)=0$ and the zero-dimensional eigenvalues form the discrete part of the spectrum.

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

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

where $M_i(t)\in\mathbb{C}[t]^{m\times n}$.

Definition 46. The generalized companion matrices $A(t),B(t)$ of the matrix $M(s,t)$ are the matrices with coefficients in $\mathbb{C}[t]$ of size $((d-1)m+n)\times dm$ that are given by

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

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

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

We have the following interesting property that follows from a straightforward computation.

Proposition 47. *With the above notation, for all $s\in\mathbb{C}$ and all vector $v\in\mathbb{C}[t]^m$ we have*

$$M^t(s,t)v=0\Leftrightarrow(A(t)-sB(t))\begin{pmatrix} v\\ tv\\ \vdots\\ t^{d-1}v\end{pmatrix}=0.$$

Theorem 48. *With the above assumptions, the following equivalence holds:*

$$\operatorname{rank}M(s_0,t_0)\ \textit{drops}\Leftrightarrow\operatorname{rank}(A(t_0)-s_0B(t_0))\ \textit{drops}.$$

In the case $\operatorname{rank}M(s,t)$ *is generically full rank, the spectrum of the matrix $M(s,t)$ and the spectrum of the pencil matrix $A(t)-sB(t)$ coincide.*

By Theorem 48, we transform the computation of the spectrum of the polynomial matrix $M(s,t)$ into the computation of the spectrum of a bivariate pencil of matrices $A(t)-sB(t)$. If the matrices $A(t),B(t)$ are two square matrices, we could compute the spectrum of the polynomial matrix $M(s,t)$ as the roots of the algebraic equation $\det M(s,t)=0$. Therefore, our next task is to reduce the pencil $A(t)-sB(t)$ into a regular pencil that keeps the information we are interested in.

3.1.2 The $\Delta W - 1$ Decomposition

In this part, we present an algorithm, called the $\Delta W - 1$ decomposition, that has been introduced by Kublanovskaya in [22]. Its purpose is to transform an univariate polynomial matrix $M(t)$ into the form $[\Delta(t), 0]$ where $\Delta(t)$ is a polynomial matrix of full column rank and 0 is a zero block-matrix. Notice that the presentation of the decomposition algorithm is very hard to follow in [22]. Hereafter, we try to present it more clearly with some illustrative examples.

Suppose given a polynomial matrix $M(t)$ of size $m \times n, m \geq n$, under the form

$$\begin{aligned} M(t) =&[M_{s1}, 0, 0, \ldots, 0]t^s + [M_{s-1,1}, M_{s-1,2}, 0, \ldots, 0]t^{s-1} + \ldots \\ &+[M_{s-p+2,1}, \ldots, M_{s-p+2,p-1}, 0]t^{s-p+2} + [M_{s-p+1,1}, \ldots, M_{s-p+1,p-1}, M_{s-p+1,p}]t^{s-p+1} \\ &+[M_{s-p,1}, \ldots, M_{s-p,p-1}, M_{s-p,p}]t^{s-p} + \ldots + [M_{01}, M_{02}, \ldots, M_{0p}] \end{aligned}$$

where for each $i, i = 1, 2, \ldots, p$, the block matrices $M_{ji}, j = 0, 1, \ldots, s$ have the same size $m \times t_i$, $\sum_{i=1}^{p} t_i = n$ and 0 stands for the zero block-matrix.

Lemma 49. *If the matrix $M = [M_{s1}, M_{s-1,2}, \ldots, M_{s-p+1,p}]$ is of full column rank, the matrix $M(t)$ is of full column rank.*

Proof. Suppose that the matrix $M(t)$ is not of full column rank, there exists a polynomial vector $F(t) \in \mathbb{C}[t]^{n\times 1}$, $F(t) \neq 0$ such that $M(t)F(t) = 0$. Let $k := \max_j\{\deg_t f_i(t)\}, j = 1, 2, \ldots, n$, we have

$$F(t) = F_k t^k + F_{k-1}t^{k-1} + \ldots + F_0$$

where $F_i = (F_{i1}, F_{i2}, \ldots, F_{in})^t \in \mathbb{C}^{n\times 1}, i = 0, 1, \ldots, k$ and $F_k \neq 0$. From

$$\begin{aligned} M(t)F(t) = 0 = &[M_{s1}, 0, 0, \ldots, 0]F_k t^{s+k} + ([M_{s-1,1}, M_{s-1,2}, 0, \ldots, 0]F_k + [M_{s1}, 0, 0, \ldots, 0]F_{k-1})t^{s+k-1} \\ &+ ([M_{s1}, 0, 0, \ldots, 0]F_{k-2} + [M_{s-1,1}, M_{s-1,2}, 0, \ldots, 0]F_{k-1} + [M_{s-2,1}, M_{s-2,2}, M_{s-2,3}, \ldots, 0]F_k)t^{s+k-2} \\ &+ \ldots + [M_{01}, M_{02}, \ldots, M_{0p}]F_0 \end{aligned}$$

for every $t \in \mathbb{C}$, we deduce that the coefficients of the matrix $M(t)F(t)$ are zero matrices. By the independence of the columns of the matrix $M = [M_{s1}, M_{s-1,2}, \ldots, M_{s-p+1,p}]$, we obtain

$$\begin{aligned} &F_{k1} = F_{k2} = \ldots = F_{k,t_1} = 0, \\ &F_{k,t_1+1} = F_{k,t_1+2} = \ldots = F_{k,t_1+t_2} = F_{k-1,1} = F_{k-1,2} = \ldots = F_{k-1,t_1} = 0 \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned}$$

Thus, the vector coefficient F_k is null which gives a contradiction. □

Corollary 50. *Let*

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

be an univariate polynomial matrix of size $m \times n$ $(m \geq n)$. If M_s is of full column rank then $M(t)$ is of full column rank.

Suppose given an univariate polynomial $m \times n$ matrix of rank ρ and degree $s \geq 1$ with $m \times n$ constant matrices $M_0, M_1, \ldots, M_s$

$$M(t) = t^s M_s + t^{s-1} M_{s-1} + \ldots + M_0.$$

The decomposition of $M(t)$ under the form

$$M(t)W(t) = [\Delta(t), 0] \tag{3.1.2}$$

is called the $\Delta W - 1$ decomposition, where $W(t)$ is an $n \times n$ unimodular polynomial matrix, $\Delta(t)$ is an $m \times \rho$ polynomial matrix of full column rank whose degree does not exceed s, 0 is an $m \times (n - \rho)$ zero matrix. The $\Delta W - 1$ decomposition algorithm computes the sequence of polynomial matrices $M_0(t) = M(t), M_1(t), \ldots, M_l(t)$ where $M_l(t) = [\Delta(t), 0]$ and $M_k(t) = M_{k-1}(t)W_k(t)$, $W_k(t)$ is an unimodular matrix, $k = 1, 2, \ldots, l$.

Now, we are ready to describe the $\Delta W - 1$ decomposition algorithm:

Step 1 Construct an auxiliary matrix N_1 as follows.

(i) if all the columns of M_s are nonzero then $N_1 := M_s$. Otherwise, M_s contains some zero columns. By column permutations, we can transform M_s into $M_s^* := [\bar{M}_{s1}, 0]$ where $\bar{M}_{s1}$ is the nonzero columns of M_s of size $m \times t_1$, so the coefficient matrices M_q are permuted with the form $M_q^* := [M_{q1}, M_{q2}], q = s - 1, \ldots, 0$ where M_{q1}, M_{q2} are respectively the $m \times t_1$ and $m \times (n - t_1)$.

(ii) If all the columns of $M_{s-1,2}$ are nonzero, then

$$N_1 := [\bar{M}_{s1}, M_{s-1,2}].$$

Otherwise, the columns of the coefficient matrices $M_{q2}, q = s-1, .., 0$ can be permuted to get $M_{s-1,2}^* := [\bar{M}_{s-1,2}, 0]$ where $\bar{M}_{s-1,2}$ is the nonzero columns of $M_{s-1,2}$ of size $m \times t_2$ and $M_{q2}^* := [M_{q2}, M_{q3}], q = s-2, \ldots, 0$. The blocks M_{q2}, M_{q3} are respectively of size $m \times t_2$ and $m \times (n - t_1 - t_2)$.

(iii) if all the columns of $M_{s-2,3}$ are nonzero, then

$$N_1 := [\bar{M}_{s1}, \bar{M}_{s-1,2}, M_{s-2,3}]$$

Otherwise, the above process will be repeated and it terminates after $p \leq s + 1$ steps where an $m \times n$ matrix N_1 of the form

$$N_1 := [\bar{M}_{s1}, \bar{M}_{s-1,2}, \bar{M}_{s-2,3}, \ldots, \bar{M}_{s-p+2,p-1}, M_{s-p+1,p}]$$

consisting in $m \times t_1, m \times t_2, \ldots, m \times t_{p-1}$ and $m \times (n - \delta_{p-1})$ block-matrices respectively with $\delta_k := \sum_{i=1}^{k} t_i$.

(iv) If $p < s + 1$, then all the columns of N_1 are nonzero. If $p = s + 1$, the last columns of N_1 may be zero columns. In this case, the size of the matrix polynomial transformed of $M(t)$ can be reduced by deleting zero columns and thus, we obtain the polynomial

matrix $M'(t)$ of smaller size. Denoting the size of this newly constructed polynomial matrix by $m \times n_1, (n_1 \leq n_0 := n)$, we have

$$N_1 := [\underbrace{\bar{M}_{s1}}_{t_1}, \underbrace{\bar{M}_{s-1,2}}_{t_2}, \ldots, \underbrace{\bar{M}_{s-p+2,p-1}}_{t_{p-1}}, \underbrace{\bar{M}_{s-p+1,p}}_{t_p}]$$

where $\sum_{i=1}^{p} t_i = n_1$ and all the columns of N_1 are nonzero columns.

Step 2 If N_1 is of full column rank, then $\Delta(t) = M'(t)$ because $M'(t)$ is of full column rank (Lemma 49). The algorithm stops here. Otherwise, find an $n_1 \times (n_1 - r_1)$ matrix T_1 whose columns form a basis of the right null space of the matrix N_1 ($r_1 := \operatorname{rank} N_1$).

Step 3 The matrix T_1 is transformed into a lower triangular form L_1 of size $n_1 \times h_1,\ h_1 \geq n_1 - r_1$ without permuting the rows such that the columns of L_1 contain a basis of the null space of the matrix N_1 and possibly, a number of columns of the identity matrix. The process obtaining the matrix L_1 from T_1 can be described in the following way. In the case the leading minor of size $n_1 - r_1$ of the matrix T_1 is not equal to zero, we obtain L_1 of size $n_1 \times (n_1 - r_1)$ by transformations of elementary orthogonal matrices (plane rotation or reflection matrices) or gaussian elimination. In the case the leading minor of size $n_1 - r_1$ of matrix T_1 is equal to zero, in the process that transforms T_1 into L_1, there exits a transposed matrix that contains an i-th row which is a zero row. We add to the matrix L_1 the corresponding column $e_i = (0, 0, \ldots, 0, \underbrace{1}_{i}, 0, \ldots, 0)$. The reduction to L_1 will be continued for the transformed matrix of smaller size by deleting its zero row.

$$L_1 = \begin{pmatrix} \ddots & 0 & \ldots & 0 \\ * & \ddots & 0 & 0 \\ \ldots & \ldots & \ddots & 0 \\ \ldots & \ldots & \ldots & \ddots \\ \ldots & \ldots & \ldots & \ldots \\ * & * & * & * \end{pmatrix}$$

For the following steps, we can assume for simplicity that L_1 is of size $n_1 \times (n_1 - r_1)$. Notice that if $h_1 > n_1 - r_1$, we only replace everywhere the number $n_1 - r_1$ with h_1 and an identity matrix I_{r_1} with $I_{n_1 - h_1}$.

The matrix L_1 is written in block-matrix as follows:

(i) If $\delta_{k-1} \leq n_1 - r_1, \delta_k > n_1 - r_1$ for $k \leq p - 1$ then L_1 has the form

$$L_1 = \begin{matrix} t_1\{ \\ t_2\{ \\ \vdots \\ t_k\{ \\ \vdots \\ t_p\{ \end{matrix} \begin{pmatrix} L_{11} & 0 & \ldots & \ldots & 0 \\ L_{21} & L_{22} & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots & 0 \\ L_{k1} & L_{k2} & \ldots & \ldots & L_{kk} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \underbrace{L_{p1}}_{t_1} & \underbrace{L_{p2}}_{t_2} & \ldots & \ldots & \underbrace{L_{pk}}_{t'_k} \end{pmatrix} \tag{3.1.3}$$

where $L_{ii}, i = 1, 2, \ldots, k-1$ are nonsingular lower triangular matrices of size $t_i \times t_i$, L_{pk} is a lower triangular matrix of size $t_k \times (n_1 - r_1 - \delta_{k-1})$ and of full column rank.

(ii) If $\delta_{k-1} \leq n_1 - r_1, \delta_k > n_1 - r_1$ only for $k = p-1$ then L_1 has the form

$$L_1 = \begin{array}{c} t_1\{ \\ t_2\{ \\ \vdots \\ t_{p-1}\{ \\ t_p\{ \end{array} \begin{pmatrix} L_{11} & 0 & \ldots & \ldots & 0 \\ L_{21} & L_{22} & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots & 0 \\ L_{p-1,1} & L_{p-2,2} & \ldots & L_{p-1,p-1} & 0 \\ \underbrace{L_{p1}}_{t_1} & \underbrace{L_{p2}}_{t_2} & \ldots & \underbrace{L_{p,p-1}}_{t_{p-1}} & \underbrace{L_{pp}}_{t'_p} \end{pmatrix} \tag{3.1.4}$$

where $L_{ii}, i = 1, 2, \ldots, p-1$ are nonsingular lower triangular matrices of size $t_i \times t_i$, L_{pp} is a lower triangular matrix of size $t_p \times (n_1 - r_1 - \delta_{p-1})$ and of full column rank.

Step 4 Construct a left triangular unimodular $n_1 \times n_1$ matrix $W^{(1)}(t)$ as a following way

(i) If L_1 has the form (3.1.3) then

$$W^{(1)}(t) = \begin{pmatrix} L_{11} & 0 & \ldots & \ldots & 0 \\ tL_{21} & L_{22} & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots & 0 \\ t^{k-1}L_{k1} & t^{k-2}L_{k2} & \ldots & L_{kk} & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ t^{p-1}L_{p1} & t^{p-2}L_{p2} & \ldots & t^{p-k}L_{pk} & I_{r_1} \end{pmatrix}$$

where I_{r_1} is an identity matrix of size $r_1 \times r_1$.

(ii) If L_1 has the form (3.1.4) then

$$W^{(1)}(t) = \begin{pmatrix} L_{11} & 0 & \ldots & \ldots & \ldots & 0 \\ tL_{21} & L_{22} & 0 & \ldots & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ t^{p-2}L_{p-1,1} & t^{p-3}L_{p-1,2} & \ldots & L_{p-1,p-1} & 0 & 0 \\ t^{p-1}L_{p1} & t^{p-2}L_{p2} & \ldots & tL_{p,p-1} & L_{pp} & I_{r_1} \end{pmatrix}$$

where I_{r_1} is an identity matrix of size $r_1 \times r_1$.

Then, we construct an unimodular polynomial matrix

$$W_1(t) = \begin{cases} W^{(1)}(t) & \text{if } n = n_1 \\ \text{diagonal}\{W^{(1)}(t), I_{n-n_1}\} & \text{if } n > n_1 \end{cases}.$$

Step 5 Obtain the matrix

$$M_1(t) = M_0(t)\Omega_1 W_1(t) = M_0^1 + tM_1^1 + \ldots + t^{s_1}M_{s_1}^1$$

where $s_1 \leq s$ and Ω_1 is the permutation matrix of the first step.

Start with $j = 1$ and repeat the above steps (1)-(5) of the algorithm for the matrix $M_j(t)$ until we obtain a matrix M_{l+1} of full column rank. In this case, we have the required $\Delta W - 1$ decomposition

$$M_l(t) = M(t)W(t) = [\Delta(t), 0]$$

where $W(t) = \prod_{i=1}^{l} \Omega_i W_i(t)$ is an $n \times n$ unimodular polynomial matrix and $\Delta(t)$ is a polynomial matrix of full column rank.

Now, we turn to the proof of the $\Delta W - 1$ decomposition algorithm.

- First, we see that the choice of the unimodular matrices $W_i(t)$ does not increase the degree of the matrix $M(t)$ under transformation. Thus, the degree of $\Delta(t)$ is not bigger than the degree of $M(t)$.

- Second, in each step k of the algorithm, it eliminates $(n_k - r_k) > 0$ vector coefficients at the greatest degree in t of the polynomial columns of the matrix $M_{k-1}(t), k = 1, 2, \ldots, l+1$ under transformation. Therefore, after a finite number of steps, the resulting matrix will have zero columns and its size can be reduced by deleting these zero columns, so that $n_k < n_{k-1}$. The matrices $M_k(t)$ and $M_{k-1}(t)$ have at least r_k identical columns whose vector coefficients at the greatest degree are linearly independent. Thus, $r_{k+1} \geq r_k$. Therefore, the number $(n_k - r_k)$ decreases in a finite number of steps of the algorithm and at the step l, $n_{l+1} - r_{l+1} = 0$. The algorithm stops here.

- Finally, we prove that the matrix $\Delta(t)$ is of full column rank. The matrix $\Delta(t)$ is written under the form

$$\begin{aligned}\Delta(t) =&[\bar{\Delta}_{s1}, 0, 0, \ldots, 0]t^s + [\Delta_{s-1,1}, \bar{\Delta}_{s-1,2}, 0, \ldots, 0]t^{s-1} + \ldots \\ &+[\Delta_{s-p+2,1}, \ldots, \bar{\Delta}_{s-p+2,p-1}, 0]t^{s-p+2} + [\Delta_{s-p+1,1}, \ldots, \Delta_{s-p+1,p-1}, \bar{\Delta}_{s-p+1,p}]t^{s-p+1} \\ &+[\Delta_{s-p,1}, \ldots, \Delta_{s-p,p-1}, \Delta_{s-p,p}]t^{s-p} + \ldots + [\Delta_{01}, \Delta_{02}, \ldots, \Delta_{0p}].\end{aligned}$$

  By construction, the matrix $N_{l+1} = [\bar{\Delta}_{s1}, \bar{\Delta}_{s-1,2}, \ldots, \bar{\Delta}_{s-p+1,p}]$ is of full column rank. By Lemma 49, the $\Delta(t)$ is of full column rank.

Remark 51. In the second chapter, we used the LU-decomposition to transform easily an arbitrary constant matrix A to a matrix under the form $[A_1|0]$ where A_1 is of full column rank. However, this algorithm can not be applied to a polynomial matrix $M(t)$ because the operations of the transformation of $M(t)$ have been done over the polynomial ring $\mathbb{C}[t]$, not the field $\mathbb{C}$. Thus, the $\Delta W - 1$ decomposition algorithm is required although it is much more complicated.

Now, we give some examples to illustrate the above algorithm.

Example 52. Let $M(t)$ be an univariate polynomial matrix

$$M(t) := \begin{pmatrix} 2t^2+3t+1 & t+1 & 2t^2+2t \\ 1 & 5t^2 & -5t^2+1 \\ 2t+1 & 3 & 2t-2 \\ t & t & 0 \end{pmatrix} = M_2t^2 + M_1t^1 + M_0$$

where

$$M_2 = \begin{pmatrix} 2 & 0 & 2 \\ 0 & 5 & -5 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, M_1 = \begin{pmatrix} 3 & 1 & 2 \\ 0 & 0 & 0 \\ 2 & 0 & 2 \\ 1 & 1 & 0 \end{pmatrix}, M_0 = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 3 & -2 \\ 0 & 0 & 0 \end{pmatrix}.$$

From all columns of the matrix M_2 are nonzero columns, we choose $N_1 := M_2$ and then the null space of N_1 is $L_1 := [1, -1, -1]^t$. So we construct the matrix

$$W^{(1)}(t) = \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ -1 & 0 & 1 \end{pmatrix}.$$

We have

$$M_1(t) = M(t)W^{(1)}(t) = \begin{pmatrix} 0 & t+1 & 2t^2+2t \\ 0 & 5t^2 & -5t^2+1 \\ 0 & 3 & 2t-2 \\ 0 & t & 0 \end{pmatrix}.$$

From the coefficient matrix of greatest degree of the matrix $\Delta(t) := \begin{pmatrix} t+1 & 2t^2+2t \\ 5t^2 & -5t^2+1 \\ 3 & 2t-2 \\ t & 0 \end{pmatrix}$ is $\begin{pmatrix} 0 & 2 \\ 5 & -5 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}$ of full column rank. By Corollary 50, the matrix $\Delta(t)$ is of full column rank.

Example 53. Let $M(t)$ be an univariate polynomial matrix

$$M(t) := \begin{pmatrix} -t & 0 & t^2 & 1+t^3 \\ 0 & -t & -1+t^3 & -t^2 \\ t^2 & 1+t^3 & t & 0 \end{pmatrix} = M_3t^3 + M_2t^2 + M_1t + M_0$$

where

$$M_3 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, M_2 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \end{pmatrix}, M_1 = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, M_0 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

From the fisrt column of the matrix M_3 is zero column, we permute the first column and the fourth column of M_3 and obtain

$$M_3^* = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix},$$

so the coefficient matrix M_2, M_1, M_0 are permuted under the form

$$M_2^* = \begin{pmatrix} 0 & 0 & 1 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, M_1^* = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, M_0^* = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

Thus $N_1 := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$. From the null space of N_1 is $[0,1,0,-1]^t$, we obtain the matrix

$$W^{(1)}(t) := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -t & 0 & 1 \end{pmatrix}.$$

Denote by $P(m,n,k)$ the square matrix of size $k \times k$ obtained by permuting the column number m with the column number n. We have

$$M_1(t) := M(t)P(1,4,4)W^{(1)}(t) = \begin{pmatrix} 1+t^3 & t^2 & t^2 & -t \\ -t^2 & -t & -1+t^3 & 0 \\ 0 & 1 & t & t^2 \end{pmatrix}.$$

Repeat the above procedure to the polynomial matrix $M_1(t)$, we obtain the matrix $N_2 := \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ and the null space of N_2 is $[1,0,-1,0]^t$. Thus,

$$W^{(2)}(t) := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ -t & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

and we obtain the matrix

$$M_2(t) := M_1(t)P(2,3,4)W^{(2)}(t) = \begin{pmatrix} t^2 & 1 & t^2 & -t \\ -1+t^3 & 0 & -t & 0 \\ t & -t & 1 & t^2 \end{pmatrix}.$$

Repeat the above procedure to the matrix $M_2(t)$, we obtain the matrix

$$W^{(3)}(t) := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & t & 0 & 1 \end{pmatrix}$$

and therefore

$$M_3(t) := M_2(t)P(1,2,4)P(2,4,4)W^{(3)}(t) := \begin{pmatrix} t^2 & 0 & t^2 & 1 \\ -1+t^3 & 0 & -t & 0 \\ t & 0 & 1 & -t \end{pmatrix}.$$

The matrix

$$\Delta(t) := \begin{pmatrix} t^2 & t^2 & 1 \\ -1+t^3 & -t & 0 \\ t & 1 & -t \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} t^3 + \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} t^2 + \begin{pmatrix} 0 & 0 & 0 \\ 0 & -1 & 0 \\ 1 & 0 & -1 \end{pmatrix} t + \begin{pmatrix} 0 & 0 & 1 \\ -1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

is of full column rank because the matrix $\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}$ is of full column rank (By Corollary 50).

3.1.3 The algorithm for extracting the regular part of a non square bivariate pencil of matrices

Now, we can give an algorithm to separate the continuous and discrete spectrum of a bivariate pencil of matrices.

Theorem 54. *An $m \times n$ pencil $M(s,t) = A(t) - sB(t)$ is equivalent to a pencil of the following form*

$$\begin{pmatrix} M_{11}(s,t) & 0 & 0 \\ M_{21}(s,t) & M_{22}(s,t) & 0 \\ M_{31}(s,t) & M_{32}(s,t) & M_{33}(s,t) \end{pmatrix} \tag{3.1.5}$$

where the pencil $M_{22}(s,t)$ is regular pencil which has only continuous spectrum coinciding with the continuous spectrum of $M(s,t)$, the pencil $M_{11}(s,t)$ of full row rank determines one-dimensional eigenvalues of the form $(0,t)$ and the pencil $M_{33}(s,t)$ of full column rank determines one-dimensional eigenvalues of the form (∞,t). The union of the discrete spectrum of the pencil $M_{11}(s,t)$ and $M_{33}(s,t)$ coincides with the discrete spectrum of $M(s,t)$.

We describe an algorithm for constructing a pencil of the form (3.1.5). Set $\rho = \operatorname{rank} A(t)$, $A_{11}(t) = A(t), B_{11}(t) = B(t)$.

Step 1

i) Transform $A_{11}(t)$ into the form $[\Delta_0(t), 0]$ by the $\Delta W - 1$ decomposition that means

$$A_{11}(t)Q_0(t) = [\Delta_0(t), 0]$$

where $Q_0(t)$ is an unimodular matrix. Then, compute

$$B_{11}(t)Q_0(t) = [\underbrace{B_1(t)}_{\rho} \mid \underbrace{B_2(t)}_{n-\rho}]$$

.

ii) Determine an unimodular matrix $P_0(t)$ such that

$$P_0(t)B_2(t) = \begin{pmatrix} \bar{B}_{11}(t) \\ \hline 0 \end{pmatrix}$$

where $\bar{B}_{11}(t)$ has full row rank. At the end of ii), matrices $A(t)$ and $B(t)$ are represented under the form

$$P_0(t)A_{11}(t)Q_0(t) = \left(\begin{array}{c|c} A_{21}(t) & 0 \\ \hline A_{22}(t) & 0 \end{array}\right), \quad P_0(t)B_{11}(t)Q_0(t) = \left(\begin{array}{c|c} B_{21}(t) & \bar{B}_{11}(t) \\ \hline B_{22}(t) & 0 \end{array}\right)$$

where
- $\bar{B}_{11}(t)$ has full row rank.
- $\begin{pmatrix} A_{21}(t) \\ \hline A_{22}(t) \end{pmatrix}$ has full column rank.

We have

$$P_0(t)(A_{11}(t) - sB_{11}(t))Q_0(t) = \left(\begin{array}{c|c} A_{21}(t) - sB_{21}(t) & -s\bar{B}_{11}(t) \\ \hline A_{22}(t) - sB_{22}(t) & 0 \end{array}\right)$$

iii) By the permutation of block rows, we obtain the matrix

$$PP_0(t)(A_{11}(t) - sB_{11}(t))Q_0(t) = \left(\begin{array}{c|c} A_{22}(t) - sB_{22}(t) & 0 \\ \hline A_{21}(t) - sB_{21}(t) & -s\bar{B}_{11}(t) \end{array}\right)$$

where P is a matrix of this permutation.

Step 2 If the matrix $A_{22}(t)$ is not of full column rank, we repeat the Step 1 for the pencil $A_{22}(t) - sB_{22}(t)$ until the step k where the matrix $A_{k+1,k+1}(t)$ is of full column rank. Thus, we have the pencil

$$P(t)M(s,t)Q(t) = \left(\begin{array}{c|c} A_{k+1,k+1}(t) - sB_{k+1,k+1}(t) & 0 \\ \hline A_{k+1,k}(t) - sB_{k+1,k}(t) & M_{33}(s,t) \end{array}\right)$$

where $P(t), Q(t)$ are unimodular matrices.

If the pencil of the $m_1 \times n_1$ matrix $A_{k+1,k+1}(t) - sB_{k+1,k+1}(t)$ is not regular pencil so it is not square matrix and not of full row rank, then we repeat the above procedure to the transposed pencil $A^t_{k+1,k+1}(t) - sB^t_{k+1,k+1}(t)$. For instance, the steps consist in the following operations: Set $\tilde{A}_{11}(t) = A_{k+1,k+1}(t), \tilde{B}_{11}(t) = B_{k+1,k+1}(t)$

i) Transform the transpose matrix $\tilde{B}^t_{11}(t)$ into the form $[\tilde{\Delta}_0(t), 0]$ that means

$$\tilde{B}^t_{11}(t)\tilde{Q}_0(t) = [\underbrace{\tilde{\Delta}_0(t)}_{\tilde{\rho}} \mid \underbrace{0}_{m_1-\tilde{\rho}}]$$

where $\tilde{Q}_0(t)$ is an unimodular matrix and $\tilde{\rho} = \operatorname{rank} \tilde{B}^t_{11}(t)$. Then, compute

$$\tilde{Q}^t_0(t)(\tilde{A}_{11}(t) - s\tilde{B}_{11}(t)) = \left(\begin{array}{c} \tilde{A}_2(t) - s\tilde{B}_2(t) \\ \hline \bar{A}_1(t) \end{array}\right)$$

where $\tilde{B}_2(t) = \tilde{\Delta}^t_0(t)$.

ii) Determine unimodular matrix $\tilde{P}_0(t)$ such that

$$\tilde{A}_1(t)\tilde{P}_0(t) = \left(\begin{array}{c|c} \bar{A}_{11}(t) & 0 \end{array}\right)$$

where $\bar{A}_{11}(t)$ is an $\tilde{\rho} \times \tilde{q}$ matrix of full columns rank. At the end of ii), the pencil $\tilde{A}_{11}(t) - s\tilde{B}_{11}(t)$ is represented under the form

$$Q^t_0(t)(\tilde{A}_{11}(t) - s\tilde{B}_{11}(t))\tilde{P}_0(t) = \left(\begin{array}{c|c} \tilde{A}_{21}(t) - s\tilde{B}_{21}(t) & \tilde{A}_{22}(t) - s\tilde{B}_{22}(t) \\ \hline \bar{A}_{11}(t) & 0 \end{array}\right)$$

iii) By the permutation of block columns, we obtain the matrix

$$Q^t_0(t)(\tilde{A}_{11}(t) - s\tilde{B}_{11}(t))\tilde{P}_0(t)C = \left(\begin{array}{c|c} \tilde{A}_{22}(t) - s\tilde{B}_{22}(t) & \tilde{A}_{21}(t) - s\tilde{B}_{21}(t) \\ \hline 0 & \bar{A}_{11}(t) \end{array}\right)$$

where C is a matrix of this permutation.

If the matrix $\tilde{B}_{22}(t)$ is not of full row rank, we repeat the above procedure to the pencil $\tilde{A}_{22}(t)-s\tilde{B}_{22}(t)$ until the step l where the matrix $\tilde{B}_{l+1,l+1}(t)$ is of full row rank. Hence, we obtain the regular pencil $\tilde{A}_{l+1,l+1}(t) - s\tilde{B}_{l+1,l+1}(t)$.

At the end, we obtain the following pencil equivalent to $M(s,t)$

$$P(t)M(s,t)Q(t) = \begin{pmatrix} M_{11}(s,t) & 0 & 0 \\ M_{21}(s,t) & M_{22}(s,t) & 0 \\ M_{31}(s,t) & M_{32}(s,t) & M_{33}(s,t) \end{pmatrix}$$

where $P(t), Q(t)$ are unimodular matrices.

The pencil $M_{22}(t) = \tilde{A}_{l+1,l+1}(t) - s\tilde{B}_{l+1,l+1}(t)$ is the regular pencil. The pencil

$$M_{11}(t) = \begin{pmatrix} \bar{A}_{ll}(t) & \tilde{A}_{l,l-1}(t) - s\tilde{B}_{l,l-1}(t) & \dots & \tilde{A}_{l,1}(t) - s\tilde{B}_{l,1}(t) \\ 0 & \bar{A}_{l-1,l-1}(t) & \dots & \tilde{A}_{l-1,1}(t) - s\tilde{B}_{l-1,1}(t) \\ 0 & 0 & \ddots & \vdots \\ 0 & \dots & 0 & \bar{A}_{11}(t) \end{pmatrix}$$

is of full column rank and its spectrum does not contain a continuous part of $M(s,t)$ except for the one-dimensional eigenvalue of the form (∞, s). The pencil

$$M_{33}(s,t) = \begin{pmatrix} -s\bar{B}_{kk}(t) & 0 & 0 & \dots & 0 \\ A_{k-1,k}(t) - sB_{k-1,k}(t) & -s\bar{B}_{k-1,k-1}(t) & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \dots & \vdots \\ A_{1,k}(t) - sB_{1,k}(t) & A_{1,k-1}(t) - sB_{1,k-1}(t) & A_{1,k-2}(t) - sB_{1,k-2}(t) & \dots & -s\bar{B}_{11}(t) \end{pmatrix}$$

is of full row rank and its spectrum does not contain a continuous part of $M(s,t)$ except for the one-dimensional eigenvalue of the form $(0, s)$.

Now, we give a brief sketch of proof of Theorem 54 via the algorithm 3.1.3; for more details, see [21, 22, 56].

At the Step 1-i) of the algorithm, we can separate $Q_0(t) = [Q_{01}(t), Q_{02}(t)]$ where

$$A(t)Q_{01}(t) = \Delta_0(t) \text{ and } A(t)Q_{02}(t) = 0.$$

Therefore, the columns of $Q_{02}(t)$ form a basis of right polynomial solutions of $A(t)$ and the finite spectrum of $\Delta_0(t)$ coincides with the finite spectrum of $A(t)$. At the Step 1-ii), the unimodular matrix $P_0(t)$ is written under the form $P_0(t) = \left(\frac{P_{01}(t)}{P_{02}(t)}\right)$ where

$$P_{01}(t)B_2(t) = \bar{B}_{11}(t) \text{ and } P_{02}(t)B_2(t) = 0.$$

The rows of $P_{02}(t)$ form a basis of left polynomial solutions of $B_2(t)$ and the finite spectrum of $\bar{B}_{11}(t)$ coincides with the finite spectrum of $B_2(t)$. From

$$P_0(t)(A(t) - sB(t))Q_0(t) = \left(\begin{array}{c|c} A_{21}(t) - sB_{21}(t) & -s\bar{B}_{11}(t) \\ \hline A_{22}(t) - sB_{22}(t) & 0 \end{array}\right),$$

we deduce that the two subspaces $Q_{01}(t)$ and $P_{02}^t(t)$ form a pair of *reducing subspaces* (for instance, see [21,56]) for the pencil $M(s,t) = A(t)-sB(t)$. By [21, Theorem 3.2], the union

of the corresponding spectral characteristics of the blocks $-s\bar{B}_{11}(t)$ and $A_{22}(t) - sB_{22}(t)$ gives the whole spectrum and the right and left minimal indices with respect to s of the original pencil $M(s,t)$.

Now, we give an example to illustrate the algorithm 3.1.3

Example 55. Suppose given a bivariate pencil of matrices $M(s,t) = A(s) - tB(s)$ where

$$A(s) = \begin{pmatrix} -s^3 & -s^2 & s^2 & 0 \\ s & 0 & 1 & 0 \\ -s^2 - s + 1 & -s - 1 & s & 1 \end{pmatrix}, B(s) = \begin{pmatrix} -s^2 - s & -s - 1 & s + 1 & 0 \\ s + 1 & 1 & 1 & 0 \\ 1 + 2s & 2 & -1 & 1 \end{pmatrix}.$$

Applying the $\Delta W - 1$ decomposition to the matrices $A(s)$ and $B(s)$, we can compute unimodular polynomial matrices $P_0(s), Q_0(s)$

$$P_0(s) := \begin{pmatrix} 0 & -1 & 1 \\ 0 & 2s & 1 - 2s \\ 1 & 0 & 0 \end{pmatrix}, Q_0(s) := \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 2s \\ 1 & 0 & 1 & s \\ 0 & 1 & 0 & s + 1 \end{pmatrix}$$

such that

$$A_1(s) := P_0(s)A(s)Q_0(s) = \left(\begin{array}{ccc|c} -1 + s & 1 & -2 & 0 \\ \hline 3s - 2s^2 & 1 - 2s & -1 + 4s & 0 \\ s^2 & 0 & 0 & 0 \end{array}\right)$$

$$B_1(s) := P_0(s)B(s)Q_0(s) = \left(\begin{array}{ccc|c} -2 & 1 & -1 & 1 \\ \hline -1 + 4s & 1 - 2s & 1 + 2s & 0 \\ s + 1 & 0 & 0 & 0 \end{array}\right).$$

Therefore, we obtain the matrices $A_2(s) := \begin{pmatrix} 3s - 2s^2 & 1 - 2s & -1 + 4s \\ s^2 & 0 & 0 \end{pmatrix}$ and $B_2(s) := \begin{pmatrix} -1 + 4s & 1 - 2s & 1 + 2s \\ s + 1 & 0 & 0 \end{pmatrix}$. Applying the $\Delta W - 1$ decomposition to the matrices $A_2(s)$ and $B_2(s)$, we compute the unimodular polynomial matrices $P_1(s)$ and $Q_1(s)$

$$P_1(s) := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, Q_1(s) := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 - 8s \\ 0 & 1/2 & 2 - 4s \end{pmatrix}$$

such that

$$A_3(s) := P_1(s)A_2(s)Q_1(s) = \left(\begin{array}{cc|c} 3s - 2s^2 & \frac{1}{2} & 0 \\ \hline s^2 & 0 & 0 \end{array}\right)$$

$$B_3(s) := P_1(s)A_2(s)Q_1(s) = \left(\begin{array}{cc|c} -1 + 4s & \frac{3}{2} - s & 4 - 12s + 8s^2 \\ \hline s + 1 & 0 & 0 \end{array}\right).$$

At last, we can transform the pencil of matrices $M(s,t)$ into the matrix form

$$\left(\begin{array}{c|ccc} -1 + s & 1 & -2 & 0 \\ 3s - 2s^2 & \frac{1}{2} & 0 & 0 \\ \hline s^2 & 0 & 0 & 0 \end{array}\right) - t \left(\begin{array}{c|ccc} -2 & 1 & -1 & 1 \\ -1 + 4s & \frac{3}{2} - s & 4 - 12s + 8s^2 & 0 \\ \hline s + 1 & 0 & 0 & 0 \end{array}\right)$$

where $M_1(s,t) := [s^2] - t[s+1]$ is a regular pencil part of the pencil matrix $M(s,t)$ and $M_2(s,t) := \begin{pmatrix} 1 & -2 & 0 \\ \frac{1}{2} & 0 & 0 \end{pmatrix} - t \begin{pmatrix} 1 & -1 & 1 \\ \frac{3}{2} - s & 4 - 12s + 8s^2 & 0 \end{pmatrix}$ of full row rank determines the discrete spectrum of $M(s,t)$. Hence, the one-dimensional eigenvalue of $M(s,t)$ is $s^2 - t(s+1)$ and the zero-dimensional eigenvalue of $M(s,t)$ is the pair $(1,1)$.

3.1.4 An algorithm for constructing the discrete spectrum

Consider $M(s,t) = A(t) - sB(t)$ an $m \times n$ $(m > n)$ pencil of full rank n that is free of continuous spectrum. Now, we present an algorithm for obtaining the discrete spectrum of $M(s,t)$.

Step 1 We construct a polynomial matrix $\Lambda(t) := [A(t), -B(t)]$ and compute a generalized eigenvalue t_* of $\Lambda(t)$.

Step 2 For each generalized eigenvalue t_*, we compute two matrices Q_-, Q_+ which are constant matrices of the first n and the last n rows of the matrix Q_* whose columns form a basis of the right null space of the constant matrix $\Lambda(t_*)$.

Step 3 We compute a generalized eigenvalue s_* of the pencil matrix $M_1(s) := Q_- - sQ_+$. Then (s_*, t_*) is a zero-dimensional eigenvalue of the pencil $M(s,t)$.

Now, we give a brief proof of the algorithm 3.1.4 (for more details, see [21, 22]). First, we construct a pencil matrix $M_1(s,t) = A_1(t) - sB_1(t)$ such that $\begin{pmatrix} B_1(t) \\ A_1(t) \end{pmatrix}$ forms a basis of the right null space of $\Lambda(t)$. Indeed,

$$M_1(s,t) = \begin{cases} W_-(t) - sW_+(t) & \text{if } t \neq t_* \\ Q_- - sQ_+ & \text{if } t = t_* \end{cases}$$

where t_* is a fixed generalized eigenvalue of the polynomial matrix $\Lambda(t)$. The matrices $W_-(t)$ and $W_+(t)$ are polynomial matrices composed of the first n and the last n rows of the matrix $W_0(t)$ whose columns form a minimal basis for the right null space of $\Lambda(t)$. The matrices Q_- and Q_+ are constant matrices composed of the first n and the last n rows of the matrix Q_* whose columns form a minimal basis for the right null space of the constant matrix $\Lambda(t_*)$. Thus, we have

- Each zero-dimensional eigenvalue (s_*, t_*) of the pencil $M_1(s,t)$ is also a zero-dimensional eigenvalue (s_*, t_*) of the pencil $M(s,t)$ and the corresponding eigenvectors x_* and y_* of the pencils $M(s,t)$ and $M_1(s,t)$ respectively satisfy the following relations:

$$x_* = Q_+ y_*, y_* = Q_*^t \begin{pmatrix} x_* \\ s x_* \end{pmatrix}.$$

- A pair (s_*, t_*) is a zero-dimensional eigenvalue of the pencil $M(s,t)$ if t_* is a generalized eigenvalue of the polynomial matrix $\Lambda(t)$ and s_* is a generalized eigenvalue

of the pencil $M_1(s, t_*)$. This property is deduced from the fact that if y_* is an eigenvector corresponding to the generalized eigenvalue s_* of the pencil $M(s_*, t_*)$ then $M(s_*, t_*)y_* \equiv (Q_- - s_*Q_+)y_* = 0$ so that y_* is also an eigenvector corresponding to the generalized eigenvalue s_* of the pencil $M_1(s, t_*)$.

Remark 56.

i) The polynomial matrix $W_0(t)$ can be computed by finding the $\Delta W - 1$ decomposition of the matrix $\Lambda(t)$, $\Lambda(t)W(t) = [\Delta(t), 0]$ where $\Delta(t)$ is of full column rank and $W(t) = [W_1(t), W_2(t)$ is an unimodular matrix. The matrices $W_1(t)$ and $W_2(t)$ are of size $2n \times \rho$ and $2n \times (2n - \rho)$, respectively ($\rho := \operatorname{rank} \Lambda(t)$). The matrix $W_2(t)$ form a basis of the right null space of $\Lambda(t)$. Then, we can find $W_0(t)$ from $W_2(t)$.

ii) The generalized eigenvalue t_* of the matrix $\Lambda(t)$ can be computed by the algorithm 2.1.3.

3.2 Decomposition of the rational surface/surface intersection locus

Suppose given an algebraic surface $\mathbf{S}_1$ represented by implicit equation $S_1(x, y, z, w) = 0$ and an algebraic surface $\mathbf{S}_2$ represented by a parameterization

$$\Psi : \mathbb{P}^2_{\mathbb{C}} \to \mathbb{P}^3_{\mathbb{C}} : (s : t : u) \mapsto (x(s, t, u) : y(s, t, u) : z(s, t, u) : w(s, t, u))$$

where $x(s, t, u), y(s, t, u), z(s, t, u), w(s, t, u)$ are homogeneous polynomials of the same degree and without common factor in $\mathbb{C}[s, t, u]$.

A standard problem in non linear computational geometry is to determine the set $\mathbf{S}_1 \cap \mathbf{S}_2 \subset \mathbb{P}^3_{\mathbb{C}}$ which is a curve in $\mathbb{P}^3_{\mathbb{C}}$ under the assumption that S_2 is not contained in S_1. One way to proceed is to compute the roots of the homogeneous polynomial

$$S_1(x(s, t, u), y(s, t, u), z(s, t, u), w(s, t, u)) \tag{3.2.1}$$

because they are in correspondence with $\mathbf{S}_1 \cap \mathbf{S}_2$ through the regular map Ψ. Observe that 3.2.1 is identically zero if and only if $\dim(\mathbf{S}_1 \cap \mathbf{S}_2) = 2$, equivalently $\mathbf{S}_1 \subset \mathbf{S}_2$ (for $\mathbf{S}_1$ is irreducible).

If $\mathbf{S}_1$ is a rational surface represented by a parameterization, then several authors (see for instance [8] and the references therein) used some *square* matrix representations, most of the time obtained from a particular resultant matrix, of $\mathbf{S}_1$ in order to compute the set $\mathbf{S}_1 \cap \mathbf{S}_2$ by means of determinant of matrix. As we have already mentioned, such square matrix representations exist only under some restrictive conditions. Hereafter, we would like to generalize this approach for non square matrix representation that can be obtained for a much larger class of rational surfaces.

So, assume that $M(x, y, z, w)$ is a matrix representation of the surface $\mathbf{S}_1$, meaning a representation of the polynomial $S_1(x, y, z, w)$. By replacing the variables x, y, z, w by the homogeneous polynomials $x(s, t, u), y(s, t, u), z(s, t, u), w(s, t, u)$ respectively, we get the matrix

$$M(s, t, u) = M(x(s, t, u), y(s, t, u), z(s, t, u), w(s, t, u))$$

and we have the following easy property:

Lemma 57. *With the above notation, for all point* $(s_0 : t_0 : u_0) \in \mathbb{P}^2_{\mathbb{C}}$ *the rank of the matrix* $M(s_0, t_0, u_0)$ *drops if and only if the point* $(x(s_0, t_0, u_0) : y(s_0, t_0, u_0) : z(s_0, t_0, u_0) : w(s_0, t_0, u_0))$ *belongs to the intersection locus* $\mathbf{S}_1 \cap \mathbf{S}_2$.

It follows that points in $\mathbf{S}_1 \cap \mathbf{S}_2$ associated to points $(s : t : u)$ such that $u \neq 0$, are in correspondence with the set of values $(s, t) \in \mathbb{C}^2$ such that $M(s, t)$ drops of rank strictly less than its row and column dimensions that means they are in correspondence with the spectrum of $M(s, t)$ which have been defined in Section 3.1. Now, we are ready to give an algorithm to solve the surface/surface intersection problems

Algorithm 5: Matrix intersection algorithm

Input: A matrix representation of a surface $\mathbf{S}_1$ and a parameterization of a rational surface $\mathbf{S}_2$.

Output: Decomposition of the intersection points of $\mathbf{S}_1$ and $\mathbf{S}_2$.

1. Compute the matrix intersection representation M(s,t).

2. Compute the generalized companion matrices A(s) and B(s) of M(s,t).

3. Compute the pencil regular matrices $M_1(s, t) = A_1(s) - tB_1(s)$*, the pencil matrices* $M_2(s, t) = A_2(s) - tB_2(s)$ *of full column rank and the pencil matrices* $M_3(s, t) = A_3(s) - tB_3(s)$ *of full row rank.*

4. Compute the determinant of $M_1(s, t)$ *and obtain the curve corresponding to the curve intersection locus* $\mathbf{S}_1 \cap \mathbf{S}_2$.

Example 58. Let $\mathbf{S}_1$ be a sphere given as the image of the parameterization

$$\phi : \mathbb{P}^2 \to \mathbb{P}^3 : (s : t : u) \mapsto (f_1 : f_2 : f_3 : f_4)$$

where

$$f_1 = s^2 + t^2 + u^2, f_2 = 2su, f_3 = 2st, f_4 = s^2 - t^2 - u^2$$

Let $\mathbf{S}_2$ be the Steiner surface which is parametrized by

$$g_1 = s^2 + t^2 + u^2, g_2 = tu, g_3 = su, g_4 = st.$$

The computation of a matrix representation of the sphere $\mathbf{S}$ gives

$$\begin{pmatrix} -y & 0 & z & x+w \\ 0 & -y & -x+w & -z \\ z & x+w & y & 0 \end{pmatrix}.$$

Now, a point P belongs to the intersection of $\mathbf{S}_1$ and $\mathbf{S}_2$ if and only if $P = (s^2 + t^2 + u^2 : tu : su : st)$ and $(s : t : u)$ is one of the generalized eigenvalues of the polynomial matrix

$$M(s, t, u) = \begin{pmatrix} -tu & 0 & su & s^2 + t^2 + u^2 + st \\ 0 & -tu & -s^2 - t^2 - u^2 + st & -su \\ su & s^2 + t^2 + u^2 + st & tu & 0 \end{pmatrix}.$$

In the case $u = 0$, we obtain the generalized eigenvalues of the matrix $M(s,t,0)$ by the ours algorithm in [43]. Now, we assume that $u \neq 0$, so the points $(s : t : u)$ are correspondence to the set of the generalized eigenvalues $(s,t) \in \mathbb{C}^2$ of the bivariate matrix $M(s,t)$

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

We have $M(s,t) = M_2t^2+M_1t+M_0$ where M_0, M_1, M_2 are respectively and the generalized companion matrices of $M(s,t)$ are

$$A(s) = \begin{pmatrix} 0 & I \\ M_0^t & M_1^t \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & s & -1 & 0 & 0 \\ 0 & 0 & s^2+1 & 0 & -1 & s \\ s & -s^2-1 & 0 & 0 & s & 1 \\ s^2+1 & -s & 0 & s & 0 & 0 \end{pmatrix}$$

$$B(s) = \begin{pmatrix} I & 0 \\ 0 & -M_3^t \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 \end{pmatrix}$$

From the fact that the polynomial matrix $A(s)$ is of full column rank, we can apply the algorithm given in Section 3.1.3 for the pencil $A^t(s) - tB^t(s)$ and obtain the pencil $A_1(s) - tB_1(s)$ where

$$A_1(s) = \left(\begin{array}{cccc|ccc} 1 & -s^3 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ \hline -s^2 & 1 & 0 & 0 & 0 & 0 & 0 \\ -s(s^2+1)+s^2 & 0 & 1 & 0 & 0 & 0 & 0 \\ s+s^2 & 0 & -1 & 1 & 0 & 0 & 0 \\ 1-s^2+s^3 & 1 & s & 0 & 0 & 0 & 0 \end{array}\right), B_1(s) = \left(\begin{array}{cccc|ccc} 0 & 0 & 1 & -s & 0 & s & 1 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ \hline s^2 & 0 & -1 & 1 & 0 & 0 & 0 \\ s^3 & 1 & -s & s & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -s^2 & s & -1 & 0 & 0 & 0 & 0 \end{array}\right).$$

The regular pencil part of $A^t(s) - tB^t(s)$ is

$$M_1(s,t) = \begin{pmatrix} -s^2 & 1 & 0 & 0 \\ -s(s^2+1)+s^2 & 0 & 1 & 0 \\ s+s^2 & 0 & -1 & 1 \\ 1-s^2+s^3 & 1 & s & 0 \end{pmatrix} - t\begin{pmatrix} s^2 & 0 & -1 & 1 \\ s^3 & 1 & -s & s \\ 1 & 0 & 0 & 0 \\ -s^2 & s & -1 & 0 \end{pmatrix}$$

Hence, $\det(M_1(s,t)) = -(s^2t^2+s^2+s^4+t^4+t^2+1)$ is the equation of the curve corresponding with $S_1 \cap S_2$ through the regular map Ψ. The pencil

$$M_2(s,t) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} - t\begin{pmatrix} 0 & s & 1 \\ 0 & -1 & 0 \end{pmatrix}$$

has no the discrete spectrum and determines one-dimensional eigenvalues of the form $(0,s)$. We recover the expected fact that the intersection $S_1 \cap S_2$ has no the isolated point.

Example 59. Let $\mathbf{S}_1$ be a sphere given as the image of the parameterization

$$\phi : \mathbb{P}^2 \to \mathbb{P}^3 : (s : t : u) \mapsto (f_1 : f_2 : f_3 : f_4)$$

where

$$f_1 = s^2 + t^2 + u^2, f_2 = 2su, f_3 = 2st, f_4 = s^2 - t^2 - u^2$$

Let $\mathbf{S}_2$ be the surface which is parametrized by

$$g_1 = s^3 + t^3, g_2 = stu, g_3 = su^2 + tu^2, g_4 = u^3.$$

The matrix representation of the sphere $\mathbf{S}$ gives

$$\begin{pmatrix} -y & 0 & z & x+w \\ 0 & -y & -x+w & -z \\ z & x+w & y & 0 \end{pmatrix}.$$

Now, a point P belongs to the intersection of $\mathbf{S}_1$ and $\mathbf{S}_2$ if and only if $P = (s^3 + t^3 : stu : su^2 + tu^2 : u^3)$ and $(s : t : u)$ is one of the generalized eigenvalues of the polynomial matrix

$$M(s,t,u) = \begin{pmatrix} -stu & 0 & su^2 + tu^2 & s^3 + t^3 + u^3 \\ 0 & -stu & -s^3 - t^3 + u^3 & -su^2 - tu^2 \\ su^2 + tu^2 & s^3 + t^3 + u^3 & st & 0 \end{pmatrix}.$$

The points $(s : t : u)$, $u \neq 0$, are correspondence to the set of the generalized eigenvalues $(s,t) \in \mathbb{C}^2$ of the bivariate matrix $M(s,t)$

$$M(s,t) = \begin{pmatrix} -st & 0 & s+t & s^3 + t^3 + 1 \\ 0 & -st & -s^3 - t^3 + 1 & -s - t \\ s+t & s^3 + t^3 + 1 & st & 0 \end{pmatrix}.$$

We have $M(s,t) = M_3 t^3 + M_2 t^2 + M_1 t + M_0$ where M_0, M_1, M_2 are respectively and the generalized companion matrices of $M(s,t)$ are

$$A(s) = \begin{pmatrix} 0 & I & 0 \\ 0 & 0 & I \\ M_0^t & M_1^t & M_2^t \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & s & -s & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & s^3 + 1 & 0 & -s & 0 & 0 & 0 & 0 \\ s & -s^3 + 1 & 0 & 1 & 0 & s & 0 & 0 & 0 \\ s^3 + 1 & -s & 0 & 0 & -1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

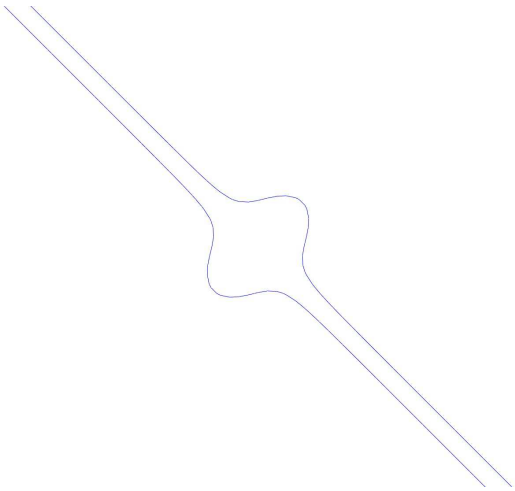


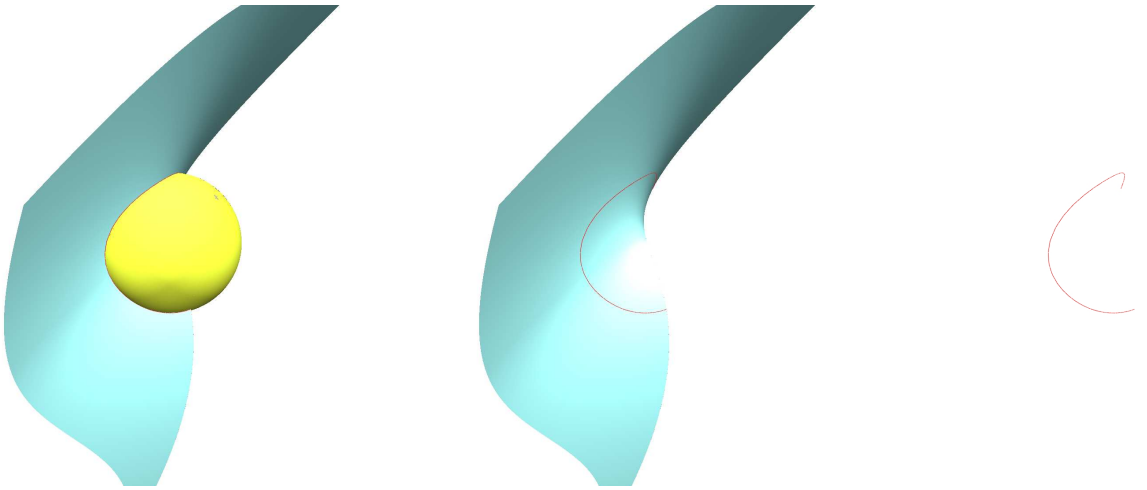
Figure 3.1: The cuvre $\mathcal{C}$ in the parameter space corresponding to $S_1 \cap S_2$

$$B(s) = \begin{pmatrix} I & 0 & 0 \\ 0 & I & 0 \\ 0 & 0 & -M_3^t \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \end{pmatrix}$$

Appling the algorithm given in Section 3.1.3 for the pencil $A^t(s) - tB^t(s)$ and obtain the regular pencil part $M_1(s,t) = A_1(s) - tB_1(s)$ where

$$A_1(s) = \begin{pmatrix} 1 & 0 & s & 0 & 1 & 0 \\ -s^3+1 & 0 & 1 & 0 & 0 & 0 \\ -s^3+1 & 0 & 0 & -s & 0 & 0 \\ 2s & 0 & 0 & 1 & s & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & -1 & 0 & 0 \end{pmatrix}, B_1(s) = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 & 0 & 0 \\ s^3 & 1 & 0 & 0 & 0 & 0 \\ -s^2 & 0 & s & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Hence, $\det(M_1(s,t)) = -s^6 - 2s^3t^3 + t^2s^2 + s^2 + 2st - t^6 + t^2 + 1$ is the equation of the curve $\mathcal{C}$ (see Figure 3.1) in the parametric space corresponding to $S_1 \cap S_2$ (see Figure 3.2) through the regular map Ψ. Remark that there are many methods to draw the intersection curve $S_1 \cap S_2$ from the curve $\mathcal{C}$ in the parametric space through the regular map Ψ (see Figure 3.3), for example see [57].



(a) (b) (c)

Figure 3.2: Intersection of the sphere S_1 and the surface S_2

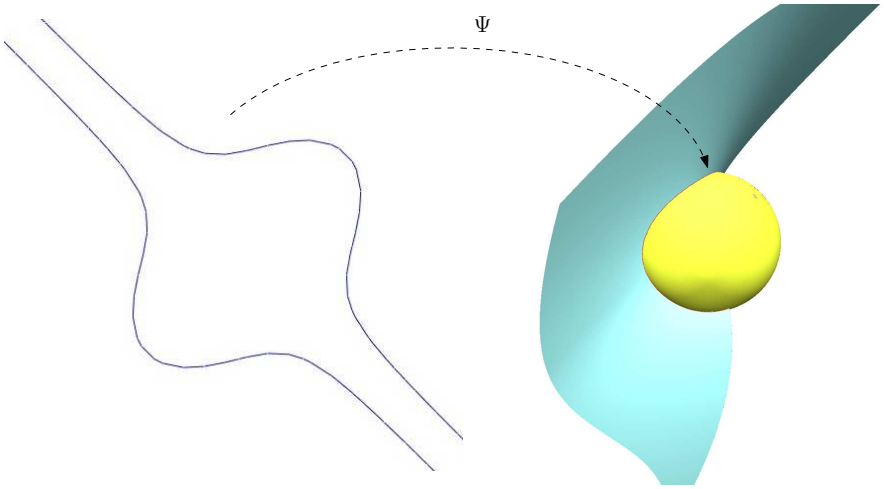


Figure 3.3: The intersection curve $S_1 \cap S_2$ through the regular map Ψ

Chapter 4

Approximate GCD of several univariate polynomials, small degree perturbations

We consider the following computational problem: given a family of generic univariate polynomials $f := (f_0, ..., f_s)$, construct an algorithm to find polynomial perturbations $u := (u_0, ..., u_s)$ with "small" degrees such that the greater common divisor of the family of polynomials $f + u$ has a "large" degree.

In this chapter, we propose an algorithm which solves this problem in polynomial time under a generic condition generalizing the normal degree sequence for the case $s = 1$.

The results in this chapter are joint work with Mohamed Elkadi and André Galligo, have been accepted for publication in [58]

Although this chapter can be seen disconnected from the rest of this thesis work, it has actually been motivated by some deep relations with tools from commutative algebra such as Hilbert function, Gröbner basis, generic initial ideal, minimal syzygies, μ-basis, etc that we encountered in our study of matrix representations of algebraic curves and hypersurfaces.

4.1 Introduction

4.1.1 A polynomial analog

The problem we address is an analog of an arithmetic question. Analogies between the ring of integers and the ring of univariate polynomials over a field proved to be often interesting.

Motivated by a cryptanalysis and using properties of continued fractions, Howgrave-Graham provided a solution to the following problem [59]: given two integers a_0 and a_1, find in polynomial time all perturbations of a fixed number of bits of a_0 and a_1 that can achieve a large GCD. The similar question for a family $a = (a_0, ..., a_s)$ of integer with $s > 1$ is much harder. Moreover, its hardness is crucial for the design of a new generation of encryption schemes, see e.g. [60] developed at MIT and IBM Research. So this question deserves much attention.

Inspired by the cited work of Howgrave-Graham, von zur Gathen et al. [23] introduced original notions of "exact" approximate GCD of univariate polynomials, building also on earlier works of numeric-symbolic computations, see e.g. [61–67] and the references therein.

More precisely, let $\mathbb{K}$ be a field and (f_0, f_1) be a pair of univariate polynomials in $\mathbb{K}[x]$ of degree at most n with a normal degree sequence in the Euclidean algorithm (this condition is generically satisfied when $\mathbb{K}$ is infinite). Let d and e be nonnegative integers such that $e < \min(2d-n, n-d)$. It is show in [23] that allowing perturbations of (f_0, f_1) by addition of a pair (u_0, u_1) of polynomials of degrees at most e then the problem of looking for a $\deg \gcd(f_0+u_0, f_1+u_1) \geq d$ has at most one solution, and if one exists, it can be computed in polynomial time. The case of more than two polynomials is left in [23] as an open question. This is precisely the problem we address in the present paper.

We divide the task in two steps: under a first condition $\mathcal{G}_1$, generically satisfied if $\mathbb{K}$ is infinite, we can reduce the problem to the case when the input polynomials have consecutive degrees, and this introduces a first limitation on the degrees of the perturbation. Then we propose a second condition $\mathcal{G}_2$, generically satisfied if the characteristic of $\mathbb{K}$ is zero, which extends the normal degree sequence condition of the case $s = 1$.

4.1.2 GCD and syzygies

We assume $\mathcal{G}_1$ and after the preprocessing, denote by n the maximum degree of the input polynomials. To benefit from concepts and results from Commutative Algebra, we homogenize the inputs in degree n (introducing a new variable y), we call them $F = (F_0, ..., F_s)$ and we consider the spanned homogeneous ideal I in $S := \mathbb{K}[x, y]$. The ring S is equipped with the lexicographical ordering on monomials and we study the corresponding Groebner basis of I.

A first natural requirement on F (generically satisfied if $\mathbb{K}$ has characteristic zero) is that the attached initial ideal $\mathrm{in}(I)$ is a gin (generic initial ideal), i.e. the stair formed by the leading exponents has steps of height 1. See section 3 and [33]. In the 2 variables setting, the combinatorial information stored by the gin is simple and is equivalent to the Hilbert function of S/I.

This point of view shows that in the case of $s + 1 > 2$ input polynomials, the degree d of the GCD is not the only natural integer invariant. The homogeneous ideal I admits a minimal resolution of length 2 and the degrees of the s minimal syzygies between $F_0, \ldots, F_s$ also appear as important numbers; we denote their ordered sequence by $m := (m_1, ..., m_s)$.

Let us mention that in Computer Aided Geometric Design, the syzygies (with $s = 2$) are used to compute the implicit equation of the projective plane curve given by the parametrization (F_0, F_1, F_2) of degree n; it is proved that the generic value for m_1 is $\lfloor \frac{n-d}{2} \rfloor$ and that $m_1 + m_2 = n - d$, where d is the degree of $\gcd(F_0, F_1, F_2)$. See e.g. [15, 42] and the references therein.

We extend these properties as follows. Given 3 integers n, $d < n$ and s, we denote by μ and t the quotient and the remainder of the division of $n - d$ by s: $\mu = \lfloor \frac{n-d}{s} \rfloor$. Then the generic set of values for $(m_1, ..., m_s)$ is $m_1 = \mu, ..., m_{s-t} = \mu, m_{s-t+1} = \mu + 1, ..., m_s = \mu + 1$, so $m_1 + \cdots + m_s = n - d$. The condition $\mathcal{G}_2$ requires that the sequence m takes this generic value, see subsection 4.3.3.

We ask for perturbations $(u_0, ..., u_s) \in \mathbb{K}[x]^{s+1}$ of degrees at most e (negative degrees means the zero polynomial) so that the perturbed polynomials $f_0 + u_0, \ldots, f_s + u_s$ have a GCD of a fixed degree d. In the homogenized setting they will be represented by homogeneous polynomials $U_0, ..., U_s$ of total degree n which are multiples of y^{n-e}. Then we consider

the set

$$\mathcal{U} = \{(u_0, \ldots, u_s) \in \mathbb{K}[x]^{s+1} : \deg u_i \leq e, \deg \gcd(f_0 + u_0, \ldots, f_s + u_s) = d\}. \quad (4.1.1)$$

The usual Euclidean division naturally extends to homogenized polynomials and gives rise to the pseudo-division with respect to the lexicographical ordering: quotients and remainders are just multiplied by suitable powers of the homogenization variable y.

In section 4, for our setting, we generalize the EEA (Extended Euclidean Algorithm) to compute, via remainders of pseudo-divisions, a reduced Groebner basis of I.

4.1.3 A recognition strategy

It is recalled in [23] that the first quotients in the EEA depend only on the top coefficients of the input polynomials; this allows a strategy of recognition where the first quotients should be identical for the inputs and their small perturbations. We make the same remark for the Hilbert function of the homogeneous ideal I, or equivalently for the generic initial ideal $\mathrm{gin}(I)$.

In [23], the authors noticed that the GCD of two polynomials has a large degree if and only if the last remainder (in the normal degree sequence) vanishes, and then they forced this vanishing for the perturbed data. In our setting, the situation is more complicated since we need to control not only one but several minimal syzygies which correspond to the vanishing of several remainders. Roughly speaking, after forcing the vanishing of the first syzygy by a first perturbation, we are led to compute the GCD of the last nonzero remainders. The cascade of perturbations is very intricate in the more general case. To bypass this difficulty, we introduce a generic condition $\mathcal{G}_2$: it allows to force simultaneously the vanishing of s consecutive remainders, and get necessary conditions on the perturbations. Then we are ready for generalizing the approach presented in [23].

The paper is organized as follows. In section 2, we present the preprocessing step. In section 3, we present the needed facts on Hilbert functions, minimal free resolutions, generic initial ideal and generic stairs. In section 4, we give our generalization of the EEA. In section 5, we describe our recognition algorithm. In section 6, we illustrate our approach on two simple examples.

4.2 Preprocessing

Let s be a positive integer, $\mathbb{K}$ be a field of characteristic zero. The following lemma is straightforward.

Lemma 60. *Given a sequence n of positive integers $n_0 \geq \cdots \geq n_s$, there exists a unique maximal decreasing sequence n of integers $q(n) = (q_0, \ldots, q_s)$ such that $q_0 = n_0$ and $q_i \leq n_i$ for $1 \leq i \leq s$, and a unique maximal integer $p = \theta(n)$ such that $p - i \leq q_i \leq n_i$ for $0 \leq i \leq s$.*

We have $p - s = q_s$.

We also denote by $\pi(n)$ the integer $\max_i(q_{i-1} - q_i, i = 1 \ldots s)$.

Example 61. If $s = 6$, $n_0 = 10$, $n_1 = n_2 = n_3 = 8$, $n_4 = 7$, $n_5 = n_6 = 2$, then $q_0 = 10$, $q_1 = 8$, $q_2 = 7$, $q_3 = 6$, $q_4 = 5$, $q_5 = 2$, $q_6 = 1$, $p = 7$, and $\pi(n) = 3$.

Lemma 62. *Given a generic family of $s+1$ polynomials $f = (f_0, \ldots, f_s)$ in $\mathbb{K}[x]$ of degrees $n_0 \geq \cdots \geq n_s$. There exists a family of $s+1$ polynomials $\phi = (\phi_0, \ldots, \phi_s)$ in $\mathbb{K}[x]$ of degrees $p, \ldots, p-s$ respectively, with $p = \theta(n)$, such that*

$$\begin{pmatrix} \phi_0 \\ \vdots \\ \phi_s \end{pmatrix} = U \begin{pmatrix} f_0 \\ \vdots \\ f_s \end{pmatrix},$$

where U is an invertible matrix in $\mathbb{K}[x]$ whose entries are polynomials of degrees bounded by $\pi(n)$.

Proof. We first compute a family of $s+1$ polynomials $g = (g_0, ..., g_s)$ of decreasing degrees $q_0 > \cdots > q_s$ such that $g_0 = f_0$ and

$$\begin{pmatrix} g_0 \\ \vdots \\ g_s \end{pmatrix} = A \begin{pmatrix} f_0 \\ \vdots \\ f_s \end{pmatrix},$$

where A is an invertible matrix in $\mathbb{K}$. To do so, we update a family g of $s+1$ polynomials of degrees $k_0 \geq \cdots \geq k_s$, starting from $g := f$ and performing the following iterations: for $0 \leq i \leq s$, if $k_{i+1} = k_i$ then $g_{i+1} := \mathrm{lt}(g_{i+1})g_i - \mathrm{lt}(g_i)g_{i+1}$. After each step we order and re-index g by degrees. The genericity of the input polynomials implies that $k_{i+1} = \deg(g_{i+1}) = k_i - 1$.

Now, we consider the vector space E spanned by g_0 and the set

$$A := \bigcup_{i=1}^{s} \{x^j g_i,\ 0 \leq j < q_{i-1} - q_i\}.$$

Then E contains $s+1$ polynomials $\phi_0, \ldots, \phi_s$ of degrees $p, \ldots, p-s$ respectively. Moreover, there exists an invertible matrix V in $\mathbb{K}[x]$ whose entries are polynomials of degrees bounded by $\pi(n)$, such that

$$\begin{pmatrix} \phi_0 \\ \vdots \\ \phi_s \end{pmatrix} = V \begin{pmatrix} g_0 \\ \vdots \\ g_s \end{pmatrix}.$$

Indeed, for each i, we consider all the integers k such that $p - i < k < q_i$ and we perform successively the Euclidean division of g_i by a suitable element of A of degree k. The last remainder will be in E, and will have degree $p - i$ by genericity. □

Remark 63. After a perturbation of $f = (f_0, \ldots, f_s)$ by $u = (u_0, ..., u_s)$ such that $\deg(u_i) < p - s - \pi(n)$, $i = 0 \ldots s$, the matrix U plays the same role as in Lemma 62.

All such perturbations of f can be detected and, as U is invertible, computed from the perturbations of ϕ respecting this degree restriction.

Definition 64. We say that $f = (f_0, \ldots, f_s)$ satisfies the condition $\mathcal{G}_1$ if the previous generic conditions are satisfied.

This implies that the degree of the GCD of the family f (and of the investigated perturbed family) is at most $\pi(n) - s$. In other words, our analysis requires that starting with the input polynomials $f = (f_0, \ldots, f_s)$ and performing successive Euclidean divisions, we obtain a sequence of $s + 1$ polynomials $\phi = (\phi_0, ..., \phi_s)$ with consecutive nonnegative degrees and the unimodular transition matrix U. Moreover, we require two kinds of degree restriction on the perturbations u of f: a weak one which imposes that the degrees of the family of polynomials $v = Uu$ are bounded by $\deg(\phi_s) - 1$, and a strong one that imposes that they also satisfy the degree restriction given by the condition $\mathcal{G}_2$ in subsection 4.3.3.

4.3 Tools from Commutative Algebra

In this section we present some tools from Commutative Algebra that will be used, such as the Hilbert function, Groebner basis, generic initial ideal, and minimal syzygies.

For polynomial inputs $f_0, \ldots, f_s$ of degrees $n_0 = n, \ldots, n_s = n - s$ respectively, we denote by F_i the homogenization of f_i to degree n, I the homogeneous ideal generated by $F_0, ..., F_s$ in the Noetherian ring $S = \mathbb{K}[x, y]$ (y is the homogenization variable). We consider the reduced Groebner basis of I with respect to lexicographic ordering with $x > y$, $\mathrm{in}(I)$ is the corresponding initial monomial ideal.

The generic stairs will be used to define the condition $\mathcal{G}_2$ which extends the normal degree sequence condition in the EEA exploited in [23]. In the next section, a dehomogenization gives rise to a generalized Extended Euclidean algorithm (in the univariate setting).

4.3.1 Resolution and Hilbert Function

Let us denote by G the polynomial $\gcd(F_0, ..., F_s)$, then $g = G(x, 1)$. The (first) syzygy module of $F_0, ..., F_s$ is defined as

$$\mathrm{Syz}(F_0, ..., F_s) := \{(G_0, ..., G_s) \in S^{s+1} : \sum_{i=0}^{s} G_i F_i = 0\}.$$

For any graded S-module M, if r is an integer, we denote by $M[-r]$ the shifted graded module $\oplus_{i \in \mathbb{Z}} M_{i-r}$. We have the following well-known result.

Lemma 65. *[15] There exists an isomorphism of graded S-module*

$$\mathrm{Syz}(F_0, ..., F_s) \cong S[-m_1] \oplus \cdots \oplus S[-m_s],$$

where $(m_1, ..., m_s) \in \mathbb{N}^s, m_i \leq m_{i+1}$, $m_1 + \cdots + m_s = n - d$, $d = \deg g$.

Moreover, the $s+1$ polynomials $(F_0, ..., F_s)$ can be recovered from G and $\mathrm{Syz}(F_0, ..., F_s)$ using Hilbert-Burch Theorem (see [33, §20.4]). More precisely, let $Q_1, \ldots, Q_s$ be a basis of the free module $\mathrm{Syz}(F_0, ..., F_s)$, then the maximal minors $M_0, \ldots, M_s$ of the matrix defined by $Q_1, \ldots, Q_s$ satisfy $F_i = GM_i, i = 0 \ldots s$.

Definition 66. The Hilbert function of S/I is

$$\begin{array}{rcl} H_{S/I} : \mathbb{N} & \to & \mathbb{N} \\ u & \mapsto & H_{S/I}(u) := \dim_{\mathbb{K}}(S/I)_u. \end{array}$$

The jump function h of the Hilbert function is

$$h_{S/I}(u) := \dim_{\mathbb{K}}(S/I)_u - \dim_{\mathbb{K}}(S/I)_{u-1}.$$

Standard computations give the following results.

Lemma 67. *We have*

1. $\dim_{\mathbb{K}} S[-k]_u = \left\{ \begin{array}{c} 0, \text{ if } u < k \\ u-k+1, \text{ if } u \geq k. \end{array} \right.$
2. $H_{S/I}(u) = \dim_{\mathbb{K}} S_u - (s+1)\dim_{\mathbb{K}} S[-n]_u + \sum_{i=1}^{s} \dim_{\mathbb{K}} S[-n-m_i]_u$.
3. *The jump function h determines the s numbers $m_1, \ldots, m_s$. More precisely, if we denote by $M_1 \leq \ldots \leq M_p$ the different values of m_i and ν_i the occurrence number of M_i in the list $(m_1, \ldots, m_s)$, then*

$$h(u) = \left\{ \begin{array}{cc} 1 & \text{if } u < n, \\ -s + \nu_1 + \cdots + \nu_i & \text{if } n + M_i \leq u < n + M_{i+1}, \\ 0 & \text{if } u \geq n + M_p, \end{array} \right.$$

with $M_0 = \nu_0 = 0$.

4.3.2 Generic initial ideal, Groebner basis and generic stairs

Generic initial ideals and generic stairs (with its simple combinatorial description) were introduced and studied in Galligo's thesis [68] and then in Bayer's PhD thesis [69]. Let us present them in our setting where I is a bivariate homogeneous ideal in the polynomial ring $S = \mathbb{K}[x, y]$. Let $<$ be the lexicographical monomial ordering with $y < x$. The main result asserts that for generic triangular change of coordinates $(x = X, Y = y + \lambda x)$, the images of the ideal I have always the same initial ideal, $in(I) = \{in(f), f \in I\}$. This monomial ideal is called the generic initial ideal of I and it is denoted $\mathrm{gin}(I)$ [33]. Its diagram in $\mathbb{N}^2$ is called the generic stair.

We recall that S/I and $S/in(I)$ have the same Hilbert function [35].

Lemma 68.
1. *The stairs of a gin are closed on the left and each step has height 1 as in Figure 1.*
2. *The Hilbert function value $H_{S/I}(u)$ is equal to the number of integer points (a, b) of the line $a + b = u$ under the stairs.*

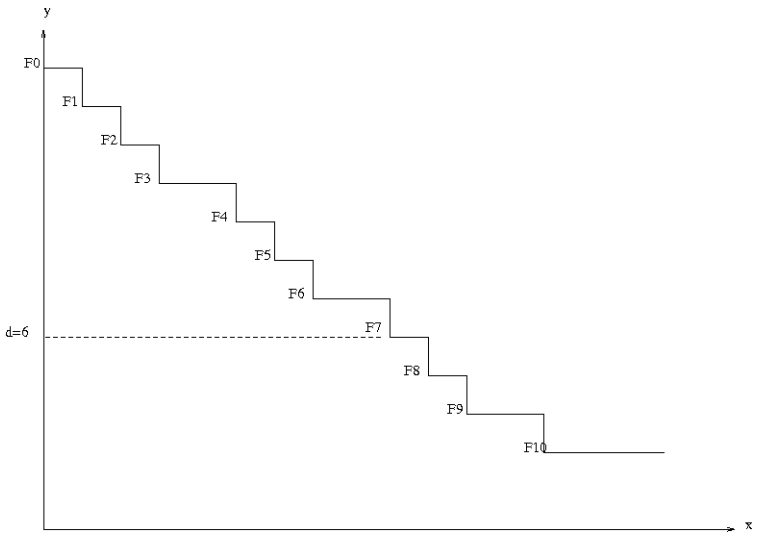


Figure 4.1: Shape of Example 2

3. *In the bivariate setting, the information described by the generic stair of I and the Hilbert function $H_{S/I}$ (or $h_{S/I}$) are equivalent.*

In the case of more than 2 variables, two ideals with distinct gins could have the same Hilbert function.

Proposition 69. *Assume that the characteristic of $\mathbb{K}$ is zero. Then for generic values in $\mathbb{K}$ of the coefficients of $F_0, ..., F_s$, the ideal $I = (F_0, ..., F_s)$ satisfies $in(I) = gin(I)$.*

Proof. Galligo's and Bayer's result can be interpreted as follows: for a fixed degree n, we denote by A the space of coefficients of $F_0, \ldots, F_s$, which is isomorphic to some $\mathbb{K}^N$. The previous change of coordinates induces a polynomial map from $A \times \mathbb{K}$ to A.

The property can be expressed by a set of nonvanishing rational conditions involving a finite number of coefficients. As $\mathbb{K}$ has characteristic zero, extending the scalars we can assume that $\mathbb{K} = \mathbb{C}$, then density w.r.t. the usual topology is equivalent to density w.r.t. Zariski topology [70]. Now for every family f, the family f_λ obtained via a triangular change of coordinates tends to f when λ tends to 0, and f_λ satisfies the required condition for almost all λ. □

4.3.3 Condition $\mathcal{G}_2$

Now we are able to translate our requirements into properties of generic the stair of I.

Proposition 70. *If I is generated by the homogeneous polynomials $F_0, \ldots, F_s$ of degree n admitting s relations of degree $m_1, \ldots, m_s$ such that $m_1 = \cdots = m_t$ and $m_{t+1} = \cdots = m_s = m_1 + 1$, then gin(I) satisfies: the s highest stairs have length 1, the following lengths are $(2, 1, \ldots, 1) \in \mathbb{N}^s$, until they reach the homogeneous degree $n + m_1 - 1$, then the lengths are equal to 2 and a series of 1 as shown in Figure 4.1. In other words the jump of the Hilbert*

function of S/I is:

$$\begin{aligned} 1 \quad &, \quad u < n \ , \\ -s \quad &, \quad n \leq u < n + m_1 \ , \\ -s+t \quad &, \quad u = n + m_1 \ , \\ 0 \quad &, \quad u > n + m_1 . \end{aligned}$$

For $s = 1$ we recover the normal degree sequence condition exploited in [23].

Definition 71. We will say that $f = (f_0, ..., f_s)$ satisfies the condition $\mathcal{G}_2$ if the initial ideal of I has the previously described shape, or equivalently that the jump of the Hilbert function of S/I is as above.

Proposition 72. *If the characteristic of $\mathbb{K}$ is zero, then the condition $\mathcal{G}_2$ is generically satisfied.*

Proof. Proposition 70 shows that generically the condition $\mathcal{G}_2$ is equivalent to the fact that, at the specified degrees, the Hilbert function of the ideal decreases by the maximal possible value $s + 1$. This property can be expressed in term of maximal rank of some minors of the matrix spanned by the multiples of f. So it is an open condition. It is generically satisfied because relying on Hilbert-Burch theorem, one can construct, for each $n - d$ and each $s < n - d$, an example where it happens. □

4.4 A generalization of the EEA

Here we present a generalization of the Extended Euclidean Algorithm (EEA) to the case of $s + 1$ polynomials $F_0, \ldots, F_s$, obtained after the preprocessing and satisfying the condition $\mathcal{G}_2$.

We construct the Groebner basis of the ideal $I = (F_0, \ldots, F_s)$ w.r.t. the lex order. Since there are only 2 variables, the completion process need not consider all the critical pairs but only the ones made by consecutive elements of the family. This boils down to performing $n - d$ pseudo-divisions as follows and we also obtain s generators of the syzygies. Assume that the initial family has been completed to $\{F_0, \ldots, F_l, \ldots, F_{l+s}\}$ with $l \geq 0$, let $k = \deg_y(F_{l+1}) - \deg_y(F_l)$ and $k = 1$ or $k = 2$. Then perform the iterated division of $y^k F_l$ by $(F_{l+1}, \ldots, F_{l+s})$:

$$y^k F_l = Q_l^1 F_{l+1} + \cdots + Q_l^s F_{l+s} + R. \tag{4.4.1}$$

If the remainder R is zero, then the previous equality defines a syzygy; while, if R is not zero, we define F_{l+s+1} to be the remainder R. The recurrence hypothesis and the condition $\mathcal{G}_2$ imply that $\deg_x(Q_l^i)$ is either 0 or 1 and then $\deg_y(F_{l+s+1}) - \deg_y(F_{l+s})$ is either 1 or 2.

We can write the equality (4.4.1) in matrix form introducing a unimodular matrix M_l such that:

$$\begin{pmatrix} F_{l+1} \\ \vdots \\ F_{l+s+1} \end{pmatrix} = \begin{pmatrix} & 1 & & \\ & & \ddots & \\ & & & 1 \\ y^k & -Q_l^1 & \ldots & -Q_l^s \end{pmatrix} \begin{pmatrix} F_l \\ \vdots \\ F_{l+s} \end{pmatrix}.$$

Dehomogenizing this construction of a Groebner basis gives rise to the following generalization of the EEA in normal degree sequence. We set $q_l^i(x) = Q_l^i(x,1)$, $f_l(x) = F_l(x,1)$ and N_l the matrix corresponding to M_l.

We assume that the preprocessing has already been performed.

Algorithm 6: GEEA (Generalized Extended Euclidean Algorithm)

Input: Polynomials $f_0, \ldots, f_s$ of degrees $n_0 = n, \ldots, n-s$, satisfying the condition $\mathcal{G}_2$.

Output: Output: A warning saying that the condition is not satisfied, or a sequence of remainders and relations expressing these reminders as combinations of the inputs.

1. Initialization: $\mathtt{N} = \mathbb{I}_{s+1}$, $a = 0$, $J = 0$.

2. For l from 0 to $n-s$ while $a = 0$ perform a multiple division

$$f_l = q_l^1 f_{l+1} + \cdots + q_l^s f_{l+s} + r.$$

   - If $r = 0$, then $a := 1$, $J := l + s$ and update $\mathtt{N}$ multiplying by the unimodular matrix N_l.
   - If $\deg(r) \neq \deg(f_{l+s}) - 1$, then send a warning and stop.
   - If $\deg(r) = \deg(f_{l+s}) - 1$, then $f_{l+s+1} := r$ and update $\mathtt{N}$ multiplying by N_l.

3. If $a = 1$, for l from $J - s + 1$ to $J - 1$, perform a multiple division $f_l = q_l^1 f_{l+1} + \cdots + q_l^J f_J + r$.

   - If $r = 0$, then update $\mathtt{N}$ multiplying by the unimodular matrix N_l.
   - If $r \neq 0$, then send a warning and stop.

   We have $\mathtt{N} \begin{pmatrix} f_0 \\ \vdots \\ f_s \end{pmatrix} = \begin{pmatrix} f_{J-s+1} \\ \vdots \\ f_J \\ 0 \end{pmatrix}$.

4. Invert the unimodular matrix $\mathtt{N}$ to get the GCD as a combination of $(f_0, ..., f_s)$ and also s generators of the syzygies.

4.5 Algorithm

For a pair (n, d) of positive integers, the restriction on the degrees e of the perturbations appearing in (1) is described by the following formula:

$$e < \min\Big(d - \lfloor \frac{n-d}{s} \rfloor, n - d\Big). \tag{4.5.1}$$

Now, we describe our algorithm to find «small» degree perturbations for the polynomials $f_0, \ldots, f_s$ to achieve a «large» degree GCD under the condition $\mathcal{G}_2$.

Algorithm 7: Construction of the set $\mathcal{U}$ defined in (4.1.1)

Input: Univariate coprime polynomials $f_0, \ldots, f_s$ of degrees $n \ldots, n-s$, satisfying the condition $\mathcal{G}_2$. Integers d, e with $d > 0$ and e as in (4.5.1).

Output: The set $\mathcal{U}$.

1. Let $F_0, \ldots, F_s$ be the homogenized polynomials to degree n of $f_0, \ldots, f_s$ respectively.

2. Apply the GEEA algorithm to $F_0, \ldots, F_s$.

3. Check the expected pattern of degrees. If not, return $\mathcal{U} = \emptyset$ or a warning.

4. We have for $1 \leq v \leq s$

$$F_{n-d+v} = \quad w_v^0 F_0 + \cdots + w_v^s F_s$$

where the w_v^j are some of the entries of the matrix P, the inverse of M_{n-d+s}. Denote the corresponding $s \times s$-minors by $D_0, \ldots, D_s$, then form

$$H_0 := F_0 \operatorname{quo} D_0 \ , \ \ldots \ , \ H_s := F_s \operatorname{quo} D_s.$$

If $H_0, \ldots, H_s$ are not associates, return $\mathcal{U} = \emptyset$.

Else, compute $U_0 := -F_0 \operatorname{rem} D_0 \ , \ \ldots \ , \ U_s := -F_s \operatorname{rem} D_s$.

5. Dehomogenize U_i and check if $\deg u_i \leq e$ for $i = 0 \ldots s$, then return $\mathcal{U} = \{(u_0, \ldots, u_s)\}$, else return $\mathcal{U} = \emptyset$.

Remark 73. Since $F_i = H_i D_i - U_i, i = 0 \ldots s$, the matrix P gives s syzygies between $F_0 + u_0, \ldots, F_s + u_s$, then we deduce from Cramer's rule that the polynomials $H_0, \ldots, H_s$ are associates.

Notation: As usual in complexity analysis, $\tilde{\mathcal{O}}$ means that we neglect log factors, see [71]. For polynomials of degrees at most n, multiplication and Euclidean division require $\tilde{\mathcal{O}}(n)$ field operations.

We recall that multiplication or inversion of invertible matrices of order s require $\mathcal{O}(s^\omega)$ field operations, $\omega < 3$.

Theorem 74. *If $f_0, \ldots, f_s$ satisfy the specification of GEEA, then the set $\mathcal{U}$ defined by (4.1.1) contains at most one element. When $\mathcal{U}$ is not empty, Algorithm 7 computes it with at most $\tilde{\mathcal{O}}(s^3 n^2)$ field operations.*

Proof. We first have to check that any $(u_0, ..., u_s)$ returned by the previous algorithm is actually in $\mathcal{U}$. If we denote by d_i (resp. h_i) the polynomial obtained dehomogenizing D_i

(resp. H_i), we have

$$\begin{aligned}\gcd(f_0+u_0,\ldots,f_s+u_s) &= \gcd(d_0h_0,\ldots,d_sh_s)\\ &= h\gcd(d_0,\ldots,d_s)=h,\end{aligned}$$

$\gcd(d_0,...,d_s)=1$ since the matrix for passing from $f_0,...,f_s$ to $f_{n-d},...,f_{n-d+s}$ is unimodular and the computation of its determinant along the first line provides a Bezout relation between its minors $d_0,...,d_s$. Then $\deg h=\deg f_0-\deg d_0=d$ and indeed $(u_0,...,u_s)\in\mathcal{U}$.

To show the correctness of the algorithm we show that $\mathcal{U}$ has at most one element, and if $\mathcal{U}\neq\emptyset$, then Algorithm 7 returns this element.

Assume that $\mathcal{U}\neq\emptyset$. Let $(u_0,...,u_s)$ in $\mathcal{U}$ and $h=\gcd(f_0+u_0,...,f_s+u_s)$, with $\deg h=d$.

For simplicity we assumed in the beginning that $d<n-s$ (Indeed, the special cases $d=n,\ldots,d=n-s$ can be treated directly along the same ideas).

Thus, from the condition on the degrees of u_i there exist uniquely determined $d_0,...,d_s$ in $\mathbb{K}[x]$ such that $f_i=d_ih-u_i$ for $i=0\ldots s$. Let $\widetilde{f_i}=f_i+u_i$ for $i=0\ldots s$ and execute the GEEA algorithm with the homogenized polynomials $\widetilde{F_0},...,\widetilde{F_s}$ of $\widetilde{f_0},...,\widetilde{f_s}$ respectively. Because of the restriction on the degrees of the perturbation, the GEEA produces the same stairs up to degree $n+m_1$, hence the sequence $m=(m_1,\ldots,m_s)$ of the degrees of the minimal syzygies of the generated ideal takes the generic value, and we obtain a unimodular matrix N such that

$$N\begin{pmatrix}\widetilde{F_0}\\ \widetilde{F_1}\\ \vdots\\ \widetilde{F_s}\end{pmatrix}=\begin{pmatrix}y^\beta H\\ 0\\ \vdots\\ 0\end{pmatrix}.$$

This implies the uniqueness property of $D_0,...,D_s$ (up to a constant). □

The cost for computing the $n-d$ generalized polynomial divisions and multiplying the inverses of the unimodular matrices in the GEEA scheme is bounded by $\tilde{\mathcal{O}}(s^3n^2)$. All other operations are not more expensive.

4.6 Examples

In the first example, we illustrate the different steps of our algorithm. In the second example, we see how we can loose uniqueness when we relax the bound on the degree of the perturbation: the GEEA scheme allows to compute an approximate GCD of degree 2, but fails to detect other approximate GCDs of degree 2. This shows that our recognition approach requires strong bounds on the degree of the perturbation.

Example 75.

$$\begin{aligned}\overline{f_0} &= x^{14}-3x^{13}+x^{11}+2x^9-3x^8-9x^7+x^6+3x^5+4x^3+x^2-2x-2,\\ f_1 &= x^{12}+x^9+2x^8+10x^7+3x^6+2x^4+7x^3+22x^2+23x,\\ f_2 &= x^{11}+x^{10}-x^8+2x^7+5x^6+5x^5+3x^4+x^2+11x+9,\\ f_3 &= x^{10}-x^9+x^8+x^7-2x^6+2x^5+x^4+4x^2-x-5.\end{aligned}$$

These polynomials are coprime, and we aim to find a perturbation (u_0, u_1, u_2, u_3) of $(\overline{f_0}, f_1, f_2, f_3)$ such that $\deg(\gcd(\overline{f_0} + u_0, f_1 + u_1, f_2 + u_2, f_3 + u_3)) = 6$.

We first perform the preprocessing to get a sequence with consecutive degrees. It amounts to replace $\overline{f_0}$ by $f_0 := \overline{f_0} - x^2 f_1$, that is

$$f_0 = -3x^{13} - 2x^{10} - 8x^9 - 6x^8 - 9x^7 - x^6 - 4x^5 - 22x^4 - 19x^3 + x^2 - 2x - 2.$$

The unimodular transition matrix V is the identity plus a matrix having only one nonzero entry, namely $-x^2$ on the first line.

Therefore, the condition $\mathcal{G}_1$ will be satisfied if the degrees of u_0, u_1, u_2, u_3 are bounded by 7, but the degree of u_1 should be bounded by 5. Here, the simplicity of V allows us to make a distinction between the degrees of the different u_i. Then we solve the problem replacing the input sequence of polynomials by (f_0, f_1, f_2, f_3) and we aim to find a perturbation (v_0, v_1, v_2, v_3) such that $\deg(\gcd(f_0+v_0, f_1+v_1, f_2+v_2, f_3+v_3)) = 6$, with $v_0 = -x^2u_1+u_0$, $v_1 = u_1,\ v_2 = u_2,\ v_3 = u_3$. Then the new data are $s = 3$, $n = 13, d = 6$, and $e < 4$.

Following Theorem 74 to achieve uniqueness, we impose that the degrees of all v_i are bounded by 3. However due to the special form of V this imposes further that $\deg(v_1) \leq 3 - 2 = 1$.

Presenting only the dehomogenized expressions, we successively compute the polynomials f_j for $j = 4, \ldots, 10$. We get

$$f_4 = -x^9 + 23x^8 - x^7 + x^6 - 2x^4 + 47x^3 + 66x^2 - x + 3,$$

$$f_5 = 67x^8 + 3x^7 + 8x^6 - 2x^4 + 147x^3 + 206x^2 + 23x + 23,$$

$$f_6 = \tfrac{10}{67}x^7 + \tfrac{384}{67}x^6 - \tfrac{29}{67}x^4 + \tfrac{88}{67}x^3 + \tfrac{106}{67}x^2 + \tfrac{702}{67}x + \tfrac{1037}{67},$$

$$f_7 = \tfrac{7988}{5}x^6 - \tfrac{523}{5}x^4 + \tfrac{1826}{5}x^3 + \tfrac{1757}{5}x^2 + \tfrac{14004}{5}x + \tfrac{21554}{5},$$

$$f_8 = -\tfrac{2}{67}x^5 + \tfrac{15719}{535196}x^4 - \tfrac{11709}{267598}x^3 - \tfrac{3543}{535196}x^2 + \tfrac{1434}{133799}x - \tfrac{2841}{133799},$$

$$f_9 = -\tfrac{222290791}{159760}x^4 - \tfrac{12672447}{15976}x^3 + \tfrac{158546991}{159760}x^2 + \tfrac{5305998}{9985}x + \tfrac{659883}{7988},$$

$$f_{10} = \tfrac{38869875}{13251185362}x^3 - \tfrac{12268325}{13251185362}x^2 - \tfrac{9935725}{13251185362}x + \tfrac{12166625}{13251185362}.$$

Figure 4.1 shows the stairs of this example.

We look for perturbations such that the perturbed f_8, f_9, f_{10} vanish. So we express them as combinations of f_0, f_1, f_2, f_3 and we get a matrix with 3 rows and 4 columns. Its 3×3-minors D_0, D_1, D_2, D_3 are polynomials of degrees 7,6,5,4 respectively.

Then (up to a sign) the polynomials $H_i = f_i \operatorname{quo} D_i, i = 0 \ldots 3$, are equal to $H = -\frac{7988}{5}x^6 - \frac{15976}{5}x - \frac{23964}{5}$, the GCD candidate.

The remainders $\operatorname{rem}(f_0, D_0) = 4x^3 + x^2 + 1$, $\operatorname{rem}(f_1, D_1) = -x$, $\operatorname{rem}(f_2, D_2) = 2x^3 - x$ and $\operatorname{rem}(f_3, D_3) = x^3 - x^2 + 1$ provide the perturbation. Theorem 74 asserts that the only solution is $\mathcal{U} = \{(-4x^3 - x^2 - 1, x, -2x^3 + x, -x^3 + x^2 - 1)\}$, which has degree $(3, 1, 3, 3)$.

Remark 76. In this example if we relax the degree bound on the perturbation to $(3,3,3,3)$ we loose uniqueness. We also observe this behavior on the following example. To be more illustrative we present the homogenized version.

Example 77.

$$f_0 = (x^2 - 2x + 3)(x^4 + x^3 + x^2 + 2x + 3) - 7 = x^6 - x^5 + 2x^4 + 4x^3 + 4x^2 + 2$$

$$f_1 = (x^2 - 2x + 3)(x^3 + 2x^2 + x - 1) + 4 = x^5 + 3x^2 + 5x + 1$$

$$f_2 = (x^2 - 2x + 3)(x^2 + 2x + 2) = x^4 + x^2 + 2x + 6.$$

These polynomials are coprime. Here $n = 6, d = 2$, then Theorem 74 applies and guaranties uniqueness if $e < 0$. With this requirement, the result of Algorithm 7 is $\mathcal{U} = \emptyset$.

However, as we constructed our example by a perturbation, we do know that with $e = 0$ there is a solution and we want to see if our algorithm detects it although the required condition on the degree is not satisfied. It will not!

Let us see what happens if we just run the process. We look for a perturbation (u_0, u_1, u_2) of (f_0, f_1, f_2) such that $\deg(\gcd(f_0 + u_0, f_1 + u_1, f_2 + u_2)) = 2$.

The corresponding homogenized polynomials to degree 6 are

$$\begin{aligned} F_0 &= x^6 - yx^5 + 2y^2x^4 + 4y^3x^3 + 4y^4x^2 + 2y^6 \\ F_1 &= yx^5 + 3y^4x^2 + 5y^5x + y^6 \\ F_2 &= y^2x^4 + y^4x^2 + 2y^5x + 6y^6. \end{aligned}$$

Applying the GEEA, we obtain

$$\begin{aligned} F_3 &= y^4x^3 - 9y^7 = yF_0 + (y - x)F_1 - 2yF_2 \\ F_4 &= y^5x^2 - y^6x - 8y^7 = yF_1 - xF_2 + F_3 \\ F_5 &= 12y^7x + 14y^8 = y^2F_2 - xF_3 - yF_4 \\ F_6 &= -\frac{23}{2}y^8 = yF_3 - (y + x)F_4 - \frac{3}{4}F_5. \end{aligned}$$

Figure 4.2 is a picture of the stairs for this example.

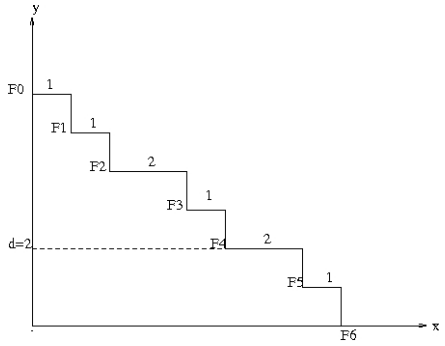


Figure 4.2: Shape of Example 3

We deduce that

$$\begin{aligned} F_5 &= -(y^2+yx)F_0 + (-2y^2+x^2)F_1 + (3y^2+3yx)F_2 \\ F_6 &= (\frac{3}{4}y^2 - \frac{1}{4}yx)F_0 + (\frac{1}{2}y^2 - 2yx + \frac{1}{4}x^2)F_1 + (-\frac{9}{4}y^2 + \frac{3}{4}yx + x^2)F_2. \end{aligned}$$

To obtain an approximate GCD of degree 2, we impose that the perturbations $\widetilde{F_5}$ and $\widetilde{F_6}$ of F_5 and F_6 vanish.

We deduce that

$$D_0 = x^4 + x^2y^2 + 3y^3x + 3y^4 \ , \ D_1 = -yx^3 - y^2x^2 \ , \ D_2 = y^2x^2 + y^3x + y^4 \ ,$$

and

$$H_0 = x^2 - yx + y^2 \ , \ H_1 = -x^2 + yx - y^2 \ , \ H_2 = x^2 - yx + y^2.$$

Since these last polynomials are associated, we set $H = x^2 - yx + y^2$. We obtain

$$\begin{aligned} U_0 &= -(F_0 \operatorname{rem} D_0) = -y^3(2x^3 + 3yx^2 - y^3) \\ U_1 &= -(F_1 \operatorname{rem} D_1) = -y^4(2x^2 + 5yx + y^2) \\ U_2 &= -(F_2 \operatorname{rem} D_2) = -y^5(2x + 5y). \end{aligned}$$

and we can verify that

$$\begin{aligned} \widetilde{F_0} &= F_0 + U_0 = H(x^4 + x^2y^2 + 3y^3x + 3y^4) \\ \widetilde{F_1} &= F_1 + U_1 = H(yx^3 + y^2x^2) \\ \widetilde{F_2} &= F_2 + U_2 = H(y^2x^2 + y^3x + y^4), \end{aligned}$$

that is $H = \gcd(\widetilde{F_0}, \widetilde{F_1}, \widetilde{F_2})$.

We conclude that the perturbation

$$(u_0, u_1, u_2) = (-2x^3 - 3x^2 + 1, -2x^2 - 5x - 1, -2x - 5)$$

of (f_0, f_1, f_2) gives the approximate GCD: $x^2 - x + 1$, which is of degree 2.

However with $v_0 = 7, v_1 = -4, v_2 = 0$, we also get the approximate GCD of degree 2, $\gcd(f_0 + v_0, f_1 + v_1, f_2 + v_2) = x^2 - 2x + 3$ which is not detected by our algorithm.

Observe that the considered perturbation changes the leading term of $\widetilde{F_4}$ while the imposed restrictions in our algorithm forbid this change.

4.7 Conclusion

In this chapter, we presented an algorithm to find small perturbations for several polynomials with a «normal degree sequence» to obtain large degree GCDs. The approach seems promising. Here are several questions and directions of research raised by our investigations.

- What is the integer analog of our process, can it be used to organize an attack on some instances of the encryption schemes cited in the introduction?

- Generalize [72] and describe the stratification (i.e the incidence relations between the strata) of the classifying space of $s+1$ polynomials defined by the sequences of degrees of the minimal syzygies.
- Describe what happens when these sequences are not generic.
- See if the degree restrictions can be weakened.

Appendix A

Implementation and example

In this appendix we show how to compute a matrix representation, μ-basis of a set of polynomial, generalized eigenvalues of a univariate polynomial matrix, intersection points of curve/curve and curve/surface, singular points of a parameterized plane curve by using the computer algebra system *Mathemagix* which are developing at INRIA Sophia Antipolis in the project GALAAD [24] and also by using the *Maple*. All these programs are included in the current distribution of Mathemagix, in the shape module *mmx/shape/mmx /matrixrepresentation* or at *http://www-sop.inria.fr/members/Luu.Ba_Thang/*. This work has been done during this thesis in parallel of the theoretical developvements. Almost algorithms are references in [4, 13, 25, 43, 53].

A.1 μ-basis of a set polynomials

In this section, we introduce a function to compute μ-basis of a set of polynomials $f := (f_0, f_1, \ldots, f_n)$ with $\gcd(f_0, f_1, \ldots, f_n) = 1$ which is defined in the first chapter.

- mubase f.
- mubase_homogeneous(f, var)

Example 78. Compute μ-basis of the set polynomials $f := [x^4 - \frac{49}{2}x^2 + \frac{115}{2}x - 33, x^4 - 25x^2 + 61x - 36, x^3 - \frac{13}{2}x^2 + \frac{27}{2}x - 8, 1]$.

- include "mubase.mmx";
- R:=QQ['x];
- f:=[$R <<$ "$x^4 - \frac{49}{2}x^2 + \frac{115}{2}x - 33$", $R <<$ "$x^4 - 25x^2 + 61x - 36$", $R <<$ "$x^3 - \frac{13}{2}x^2 + \frac{27}{2}x - 8$", $R <<$ "1"];
- mubase f

$$[[-1, 1, 0, \frac{1}{2}x^2 - \frac{7}{2}x + 3], [\frac{-15}{17}, 1, \frac{-2}{17}x - \frac{13}{17}, \frac{-15}{17}x + \frac{13}{17}],$$
$$[\frac{136}{481}x - \frac{3158}{13949}, \frac{-136}{481}x + \frac{3842}{13949}, \frac{-684}{13949}x - \frac{6418}{13949}, \frac{1274}{1073}x - \frac{17246}{13949}]]$$

Example 79. Compute μ-basis of the set polynomial $f := [x^3 + xY^2 + y^3, x^3 - x^2y, x^3 + x^2y + xy^2]$.

- include "mubase.mmx";
- R:=QQ['x,'y];
- f:=[$R << "x^3 + xY^2 + y^3", R << "x^3 - x^2y", R << "x^3 + x^2y + xy^2"$];
- var:=[R«"x",R«"y"];
- mubase_homogeneous(f,var)

$$[[2x^2 + xy, -x^2 + y^2, -x^2 - xy - y^2], [\frac{3}{2}x, \frac{-3}{2}x, \frac{-3}{2}y]]$$

A.2 Matrix representation of parameterized curve

Let $f_0, f_1, \ldots, f_n$ be n 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

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

The image of ϕ is an algebraic curve $\mathcal{C}$ in $\mathbb{P}^n_{\mathbb{K}}$ which is called a *rational* curve. Now, we give some functions to compute a matrix representation of $\mathcal{C}$ in $\mathbb{P}^2_{\mathbb{K}}$ and $\mathbb{P}^3_{\mathbb{K}}$.

- matrix_rep_curve_plane_homogeneous(curplane,varcur,varimplcurve).
- matrix_rep_curve_plane(curplane,varimplcurve).
- matrix_rep_curve_space_homogeneous(curplane,varcur,varimplcurve).
- matrix_rep_curve_space(curplane,varcur,varimplcurve)

Example 80. $(\mathcal{C}) : f_0 = s^3 + t^3, f_1 = s^2t, f_2 = s^3 + s^2t + t^3$. Then the matrix representation of $\mathcal{C}$ is

- include"curvesurface.mmx";
- R:=$QQ['s,'t,'x,'y,'z]$;
- curplane:=[$R << "s^3 + t^3", R << "s^2t", R << "s^3 + s^2t + t^3"$];
- varcur:=[$R << "s", R << "t"$];
- varimplcurve:=[$R << "x", R << "y", R << "z"$];

- matrix_rep_curve_plane_homogeneous(curplane,varcur,varimplcurve)

$$\begin{pmatrix} x-z & y & 0 \\ x & x-z & y \\ -y & 0 & x-z \end{pmatrix}$$

Example 81. $(\mathcal{C}) : f_0 = 3s^2t, , f_1 = -3s^3 + 3st^2, f_2 = st^2 + t^3, f_3 = t^3$. Then the matrix representation of $\mathcal{C}$ is

- include"curvesurface.mmx";
- R:=$QQ['s,'t,'x,'y,'z,'w]$;
- curplane:=$[R << \text{“}3s^2t\text{“}, R << \text{“} -3s^3 + 3st^2\text{“}, R << \text{“}st^2 + t^3\text{“}, R << \text{“}t^3\text{“}]$;
- varcur:=$[R << \text{“}s\text{“}, R << \text{“}t\text{“}]$;
- varimplcurve:=$[R << \text{“}x\text{“}, R << \text{“}y\text{“}, R << \text{“}z\text{“}, R << \text{“}w\text{“}]$;
- matrix_rep_curve_space_homogeneous(curplane,varcur,varimplcurve)

$$\begin{pmatrix} -y & -x-y & -z+w \\ -x+3w & -x+3z & w \end{pmatrix}$$

A.3 Matrix representation of parameterized surface

Let f_0, f_1, f_2, f_3 be homogeneous polynomials in $\mathbb{K}[s,t,u]$ of the same degree $d \geq 1$ such that their greatest common divisor (GCD) is a non-zero constant in $\mathbb{K}$. Consider a surface $\mathbf{S}$ given by parametrization

$$\begin{array}{rcl} \mathbb{P}^2_{\mathbb{K}} & \xrightarrow{\phi} & \mathbb{P}^3_{\mathbb{K}} \\ (s:t:u) & \mapsto & (f_0(s,t,u) : f_1(s,t,u) : f_2(s,t,u) : f_3(s,t,u)). \end{array}$$

Now, we give a function to compute a matrix representation of $\mathbf{S}$ in $\mathbb{P}^3_{\mathbb{K}}$.

- matrix_rep_surface(surface,varsur,varimplsur).

Example 82. Stein's Roman Surface $(\mathbf{S}) : f_0 = s^2 + t^2 + u^2, f_1 = st, f_2 = su, f_3 = tu$. Then the matrix representation of $\mathbf{S}$ is

- include"curvesurface.mmx";
- R:=$QQ['s,'t,'u,'x,'y,'z,'w]$;
- Stein:=$[R << \text{“}s^2 + t^2 + u^2\text{“}, R << \text{“}st\text{“}, R << \text{“}su\text{“}, R << \text{“}tu\text{“}]$;
- varsur:=$[R << \text{“}s\text{“}, R << \text{“}t\text{“}, R << \text{“}u\text{“}]$;
- varimplsur:=$[R << \text{“}x\text{“}, R << \text{“}y\text{“}, R << \text{“}z\text{“}, R << \text{“}w\text{“}]$;

- matrix_rep_curve_surface(surface,varsur,varimplsur)

$$\begin{pmatrix} y & y & z & w & 0 & 0 & y & 0 & 0 \\ -x & -x & 0 & 0 & w & z & -x & 0 & 0 \\ y & y & 0 & 0 & 0 & 0 & y & z & w \\ 0 & 0 & -x & -y & 0 & -y & w & 0 & y \\ 0 & z & y & 0 & -y & 0 & 0 & -y & -x \\ y & 0 & z & 0 & 0 & 0 & 0 & 0 & w \end{pmatrix}$$

A.4 Polynomial matrix and generalized eigenvalues

Suppose given a polynomial matrix $M(t) = (a_{ij}(t))$ of size $m \times n$. 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 $M_i \in \mathbb{K}^{m \times n}$.

We construct some functions to compute $M_d, M_{d-1}, \ldots, M_0$, generalized companion matrices, regular matrix and generalized eigenvalues of $M(t)$ which are defined in the second chapter.

- list_coefficients_matrix M(t).
- firstcompanionmatrix M(t).
- secondcompanionmatrix M(t).
- pencilregular(A,B) where A:=firstcompanionmatrix M(t), B:=secondcompanionmatrix M(t).
- generalized_eigenvalues M(t).

Example 83. $M := \begin{pmatrix} 3x^2 & -3x^3 + 3x \\ x + 1 & 1 \\ 2x^2 + x & x^2 + x \end{pmatrix}$

- include“pencilregular.mmx“;
- degree M

$$3$$

- list_coefficients_matrix M

$$M_3 = \begin{pmatrix} 0 & -3 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}, M_2 = \begin{pmatrix} 3 & 0 \\ 0 & 0 \\ 2 & 1 \end{pmatrix}, M_1 = \begin{pmatrix} 0 & 3 \\ 1 & 0 \\ 1 & 1 \end{pmatrix}, M_0 = \begin{pmatrix} 0 & 0 \\ 1 & 1 \\ 0 & 0 \end{pmatrix}$$

- A:=firstcompanionmatrix M;
- B:=secondcompanionmatrix M;

- pencilregular(A,B)

$$[[0],[-3]]$$

- generalized_eigenvalues M

$$[0]$$

A.5 Parameterized curve/curve intersection

Consider two curves $\mathcal{C}_1, \mathcal{C}_2$ given by parametrization

$$\begin{array}{rcl}(\mathcal{C}_1) : \mathbb{P}^1_{\mathbb{K}} & \xrightarrow{\phi_1} & \mathbb{P}^n_{\mathbb{K}} \\ (s:t) & \mapsto & (f_0(s,t) : f_1(s,t) : \cdots : f_n(s,t)).\end{array}$$

$$\begin{array}{rcl}(\mathcal{C}_2) : \mathbb{P}^1_{\mathbb{K}} & \xrightarrow{\phi_2} & \mathbb{P}^n_{\mathbb{K}} \\ (s:t) & \mapsto & (g_0(s,t) : g_1(s,t) : \cdots : g_n(s,t)).\end{array}$$

Hereafter, we give some functions to compute the intersection locus $\mathcal{C}_1 \cap \mathcal{C}_2$ in the space $\mathbb{P}^2_{\mathbb{K}}$ and $\mathbb{P}^3_{\mathbb{K}}$.

- intersection_curve_plane_homogeneous(curve1,varcur1,curve2,varcur2).
- intersection_curve_space_homogeneous(curve1,varcur1,curve2,varcur2).

In the case, the parametrization of $\mathcal{C}_1$ and $\mathcal{C}_2$ are given the univariate polynomial, we give the other functions to compute the intersection locus $\mathcal{C}_1 \cap \mathcal{C}_2$.

- intersection_curve_plane(curve1,curve2).
- intersection_curve_space(curve1,curve2).

Example 84. $(\mathcal{C}_1) : f_0 = x^4 - \frac{49}{2}x^2 + \frac{115}{2}x - 33, f_1 = x^4 - 25x^2 + 61x - 36, f_2 = x^3 - \frac{13}{2}x^2 + \frac{27}{2}x - 8, f_3 = 1.$
$(\mathcal{C}_2) : g_0 = x^3 - \frac{11}{2}x^2 + \frac{17}{2}x - 3, g_1 = x^3 - 6x^2 + 12x - 6, g_2 = x^4 - \frac{51}{2}x^2 + \frac{125}{2}x - 38, g_3 = 1.$
Then $\mathcal{C}_1 \cap \mathcal{C}_2$ are

- include “curvesurface.mmx“;
- R:=QQ[’x];
- curve1:=[$R << “x^4 - \frac{49}{2}x^2 + \frac{115}{2}x - 33“, R << “x^4 - 25x^2 + 61x - 36“, R << “x^3 - \frac{13}{2}x^2 + \frac{27}{2}x - 8“, R << “1“$];

- curve2:=[R << "$x^3 - \frac{11}{2}x^2 + \frac{17}{2}x - 3$", R << "$x^3 - 6x^2 + 12x - 6$", R << "$x^4 - \frac{51}{2}x^2 + \frac{125}{2}x - 38$", R << "1"];
- intersection_curve_space(curve1,curve2)

$$[[1, 1, 0, 1], [0, 2, 1, 1], [0, 3, 1, 1], [-308, -341, -363, 1]$$

Example 85. $(\mathcal{C}_1) : f_0 = x^3 - 3x^2y + 2xy^2 + y^3, f_1 = x^2y + 2xy^2 + 2y^3, f_2 = xy^2 + 3y^3, f_3 = y^4$.
$(\mathcal{C}_2) : g_0 = x^4 - xy^3 + y^4, g_1 = xy^3 + y^4, g_2 = xy^3 + 2y^4, g_3 = y^4$. Then $\mathcal{C}_1 \cap \mathcal{C}_2$ are

- include "curvesurface.mmx";
- R:=QQ['x,'y];
- curve1:=[R << "$x^3 - 3x^2y + 2xy^2 + y^3$", R << "$x^2y + 2xy^2 + 2y^3$", R << "$xy^2 + 3y^3$", R << "y^4"];
- curve2:= [R << "$x^4 - xy^3 + y^4$", R << "$xy^3 + y^4$", R << "$xy^3 + 2y^4$", R << "y^4"];
- varcur:=R << "x", R << "y"];
- intersection_curve_space_homogeneous(curve1,varcur,curve2,varcur)

$$[[1, 2, 3, 1], [1, 1, 2, 1]].$$

A.6 Parameterized curve/surface intersection

Consider a curve $\mathcal{C}$ given by parametrization

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

and a surface $\mathbf{S}$ by parametrization

$$\begin{array}{rcl} (\mathbf{S}) : \mathbb{P}^2_{\mathbb{K}} & \stackrel{\psi}{\rightarrow} & \mathbb{P}^3_{\mathbb{K}} \\ (s:t:u) & \mapsto & (g_0(s,t,u) : g_1(s,t,u) : g_2(s,t,u) : g_3(s,t,u)). \end{array}$$

We give a function to determinate the intersection locus $\mathcal{C} \cap \mathbf{S}$.

- intersection_curve_surface_homogeneous(surface,varsur,curve,varcur).

Example 86. A sphere $(\mathbf{S}) : f_0 = x^2 + y^2 + z^2, f_1 = 2xz, f_2 = 2xy, f_3 = x^2 - y^2 - z^2$.
A thwisted cubic: $(\mathcal{C}) : g_0 = s^3, g_1 = s^2t, g_2 = st^2, g_3 = t^3$. Then $\mathbf{S} \cap \mathcal{C}$ are

- include "curvesurface.mmx";

- R:=QQ['s,'t,'x,'y,'z];
- surface:=[$R << "x^2+y^2+z^2", R << "2xz", R << "2xy", R << "x^2-y^2-z^2"$];
- curve:=;[$R << "s^3", R << "s^2t", R << "st^2", R << "t^3"$];
- varsur:=[$R << "x", R << "y", R << "z"$;
- varcur:=[$R << "s", R << "t",$];
- intersection_curve_surface_homogeneous(surface,varsur,curve,varcur)

$$[[1,-0.73,0.54,-0.4],[1,0.73,0.54,0.4],$$

$$[1,0.54-1.03i,-0.77-1.11i,-1.56+0.19i],[1,0.54+1.03i,-0.77+1.11i,-1.56-0.19i],$$

$$[1,-0.54-1.03i,-0.77+1.11i,1.56+0.19i],[1,-0.54+1.03i,-0.77-1.11i,1.56-0.19i]]$$

A.7 Singular points of parameterized plane curve

Consider a plane curve $\mathcal{C}$ given by parametrization

$$\begin{array}{rcl}(\mathcal{C}):\mathbb{P}^1_{\mathbb{K}} & \xrightarrow{\phi} & \mathbb{P}^2_{\mathbb{K}} \\ (s:t) & \mapsto & (f_0(s,t):f_1(s,t):f_2(s,t)).\end{array}$$

We given a function to compute the singular points of $\mathcal{C}$ with its multiplicity.

- singular_point_plane(curve,varcur,int) where «int» is multiplicity of a points on $\mathcal{C}$.

Example 87. $(C): f_0 = t^5-2*t^3+2, f_1 = t^4+3, f_2 = 1$. Then $P(2,7,1)$ is of multiplicity 2 and $Q(2,3,1)$ is of multiplicity 3.

- include "singular_point.mmx";
- R:=QQ['t,'x,'y,'z];
- curve:= $[R << "t^5-2*t^3+2", R << "t^4+3", R << "1"$;
- varcur:= $[R << "t", R << "x", R << "y", R << "z"]$;
- singular_point_plane(curve,varcur,2)

$$[2,7,1],[2+8i,-1,1],[2-8i,-1,1]$$

- singular_point_plane(curve,varcur,3)

$$[[2,3,1]]$$

- singular_point_plane(curve,varcur,4)

$$[]$$

Example 88. (Chen, F and all) $(C) : f_0 = t^4 - 40 * t^3 + 40t + 1, f_1 = t^4 + 480t^2 + 1, f_2 = t^4 + 40t^3 + 480t^2 + 40t + 1$.

- include “singular_point.mmx“;
- R:=QQ[’t,’x,’y,’z];
- curve:= $[R << “t^4 - 40 * t^3 + 40t + 1“, R << “‘t^4 + 480t^2 + 1‘, R << “t^4 + 40t^3 + 480t^2 + 40t + 1“$;
- varcur:= $[R << “t“, R << “x“, R << “y“, R << “z“]$;
- singular_point_plane(curve,varcur,2)

$$[[2.4488708221968 * 10^7, 5.0600587305910 * 10^7, 7.3417921728759 * 10^7],$$
$$[7714.2545820696, 15939.828632115, 8752.0780563547],$$
$$[7.9346835678021, 16.395297170358, 23.788432278383],$$
$$[0.51773816346332, 1.0697932657153, 0.58739114339276], [1, 1, 1]]$$

- singular_point_plane(curve,varcur,3)

$$[]$$

- singular_point_plane(curve,varcur,4)

$$[]$$

A.8 Solve the equation of univariate polynomials

Let $f(x)$ be an univariate polynomial of the rational coefficients. We give a function to find all roots of $f(x)$.

- solve f(x)

Example 89. Solve the equation $x^4 + 2x + 1 = 0$.

- include “solvepolynomial.mmx“;
- f:=$QQ[’x] << “x^4 + 2x + 1“$;
- solve f;

$$[0.77184450634604 + 1.1151425080399 * i, 0.77184450634604 - 1.1151425080399 * i,$$
$$-1.0000000000000, -0.54368901269208]$$

.

Conclusion

In this thesis, we have obtained some new results following:

- Introduce a new implicit representation of rational curves of arbitrary dimensions and propose a implicit representation of rational hypersurfaces.
- Illustrate the advantages of this matrix representation by addressing several important problems of Computer Aided Geometric Design (CAGD): The intersection problem curve/curve, curve/surface and surface/surface, the point-on-curve and inversion problems, the computation of singularities of rational curves.
- Develop a symbolic/numeric algorithm to manipulate these new representations for example: the algorithm for extracting the regular part of a non square pencil of univariate polynomial matrices and bivariate polynomial matrices.
- Describes an algorithm which, given a family of generic univariate polynomials $f := (f_0, ..., f_s)$, find polynomial perturbations $u := (u_0, ..., u_s)$ with prescribed degree-bounds such that $\gcd(f_1 + u_1, ..., f_s + u_s)$ has at least a given degree, provided that such a perturbation exists in polynomial time under a generic condition generalizing the normal degree sequence
- Develop the package *matrixrepresentation* of the computer algebra system *Mathemagix* and Maple to these matrices representations.

Bibliography

[1] Laurent Busé and Marc Dohm. Implicitization of bihomogeneous parametrizations of algebraic surfaces via linear syzygies. In *ISSAC 2007*, pages 69–76. ACM, New York, 2007.

[2] Laurent Busé, David Cox, and Carlos D'Andrea. Implicitization of surfaces in $\mathbb{P}^3$ in the presence of base points. *J. Algebra Appl.*, 2(2):189–214, 2003.

[3] David Cox, Ronald Goldman, and Ming Zhang. On the validity of implicitization by moving quadrics of rational surfaces with no base points. *J. Symbolic Comput.*, 29(3):419–440, 2000.

[4] Laurent Busé and Marc Chardin. Implicitizing rational hypersurfaces using approximation complexes. *J. Symbolic Comput.*, 40(4-5):1150–1168, 2005.

[5] Laurent Busé and Jean-Pierre Jouanolou. On the closed image of a rational map and the implicitization problem. *J. Algebra*, 265(1):312–357, 2003.

[6] L. Busé, M. Chardin, and with appendix of J. Oesterlé Aron Simis. Elimination and nonlinear equations of rees algebras. *Journal of Algebra*, 324(3):1314–1333, 2010.

[7] T.W. Sederberg and F. Chen. Implicitization using moving curves and surfaces. In *Proceedings of SIGGRAPH*, volume 29, pages 301–308, 1995.

[8] Dinesh Manocha and John Canny. A new approach for surface intersection. In *Proceedings of the first ACM symposium on Solid modeling foundations and CAD/CAM applications*, pages 209–219, Austin, Texas, United States, 1991. ACM.

[9] Nicolás Botbol, Marc Dohm, and Alicia Dickenstein. Matrix representations for toric parametrizations. *Computer Aided Geometric Design*, 7:757–771, 2009.

[10] Laurent Busé, Marc Chardin, and Jean-Pierre Jouanolou. Torsion of the symmetric algebra and implicitization. *Proceedings of the American Mathematical Society*, 137(06):1855–1865., February 2009.

[11] T. Garrity and J. Warren. On computing the intersection of a pair of algebraic surfaces. *Comput. Aided Geom. Design*, 6 (2):137–153, 1989.

[12] E. Fortuna, P. Gianni, and B. Trager. Generators of the ideal of an algebraic space curve. *J. Symbolic Comput*, 44 (9):1234–1254, 2009.

[13] N. Song and R. Goldman. μ-bases for polynomial systems in one variable. *Comput. Aided Geom. Design*, 26 (2):217–230, 2009.

[14] X. Jia, H. Wang, and R. Goldman. Set-theoretic generators of rational space curves. *Journal of Symbolic Computation*, 45 (4):414 – 433, 2010.

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

[16] D. A. Aruliah, Robert M. Corless, Laureano Gonzalez-Vega, and Azar Shakoori. Geometric applications of the bezout matrix in the lagrange basis. In *Proceedings of the 2007 international workshop on Symbolic-numeric computation*, pages 55–64, London, Ontario, Canada, 2007. ACM.

[17] Laurent Busé, Houssam Khalil, and Bernard Mourrain. Resultant-based methods for plane curves intersection problems. In *Computer algebra in scientific computing*, volume 3718 of *Lecture Notes in Comput. Sci.*, pages 75–92. Springer, Berlin, 2005.

[18] H. Wang, X. Jia, and R. Goldman. Axial moving planes and singularities of rational space curves. *Comput. Aided Geom. Design*, 26 (3):300–316, 2009.

[19] H.-S. Heo, M. S. Kim, and G. Elber. The intersection of two ruled surfaces. *Computer-Aided Design*, 31(1):33–50, 1999.

[20] M. Fioravanti, L. Gonzalez-Vega, and I. Necula. Computing the intersection of two ruled surfaces by using a new algebraic approach. *Journal of Symbolic Computation*, 41 (11):1187 – 1205, 2006.

[21] V.N. Kublanovskaya and V.B. Khazanov. Spectral problems for pencils of polynomial matrices. methods and algorithms. v. *Journal of Mathematical Sciences*, 79(3):1048–1076, 1996.

[22] V.N. Kublanovskaya. Methods and algorithm of solving spectral problems for polynomial matrices and rational matrix. *Journal of Mathematical Sciences*, 96(3):3085–3287, 1999.

[23] J. von zur Gathen, M. Mignotte, and I. E. Shparlinski. Approximate polynomial gcd: Small degree and small height perturbations. *Journal of Symbolic Computation*, 45:879–886, 2010.

[24] The software mathemagix. Available at http://www.mathemagix.org.

[25] L. Busé and T. Luu Ba. Matrix-based implicit representations of algebraic curves and applications. *Computer Aided Geometric Design*, 27(9):681–699, 2010.

[26] Amit Khetan and Carlos D'Andrea. Implicitization of rational surfaces using toric varieties. *J. Algebra*, 303(2):543–565, 2006.

[27] C. D'Andrea. Resultant and moving surfaces. *Journal of Symbolic Computation*, 31:585–602, 2001.

[28] L. Busé and M. Chardin. Implicitizing rational hypersurfaces using approximation complexes. *Journal of Symbolic Computation*, 40:1150–1168, 2005.

[29] A. Simis and W.V. Vasconcelos. The syzygies of the conormal module. *Amer. J. Math*, 103:203–224, 1981.

[30] W.V. Vasconcelos. *Arithmetic of Blowup Algebras*. In London Mathematical Society Lecture Note Series vol 195. Cambridge University Press.

[31] W. Bruns and J. Herzog. *Cohen-Macaulay rings*. Cambridge studies in advanced mathematics 39. Cambridge university press 1993.

[32] M. Dohm. Implicitization of rational ruled surfaces with μ-bases. *Journal of Symbolic Computation*, 5:479–489, 2009.

[33] D. Eisenbud. *Commutative algebra with a view toward algebraic geometry*. Vol 150. Springer-Verlag, New York.

[34] Joe Harris. *Algebraic Geometry. A first course*. Graduate Texts in Mathematics 133. Apringer-Verlag NewYork, Inc 1992.

[35] D. Cox, J. Little, and D. O'Shea. *Ideals, varieties, and algorithms*. 2nd Edition. Springer-Verlag, New York, Undergraduate Texts in Mathematics.

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

[37] J. P. Jouanolou. Idéaux résultants. *Adv. in Math*, 37 (3):212–238, 1980.

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

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

[40] L. Busé and R. Goldman. Division algorithms for Bernstein polynomials. *Comput. Aided Geom. Design*, 25 (9):850–865, 2008.

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

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

[43] T. Luu Ba, L. Busé, and B. Mourrain. Curve/surface intersection problem by means of matrix representation. In *SNC'09: Proceedings of the International Conference on Symbolic Numeric Computation. Kyoto, Japan.ACM, NewYork, USA*, pages 71–78, August 2009.

[44] F. R. Gantmacher. *Théorie des matrices. Tome 2: Questions spéciales et applications*. Traduit du Russe par Ch. Sarthou. Collection Universitaire de Mathématiques, No. 19. Dunod, Paris, 1966.

[45] Gene H. Golub and Charles F. Van Loan. *Matrix computations*. Johns Hopkins Studies in the Mathematical Sciences. Johns Hopkins University Press, Baltimore, MD, third edition, 1996.

[46] F. R. Gantmacher. *Théorie des matrices. Tome 1: Théorie générale*. Traduit du Russe par Ch. Sarthou. Collection Universitaire de Mathématiques, No. 18. Dunod, Paris, 1966.

[47] Paul Van Dooren and Patrick Dewilde. The eigenstructure of an arbitrary polynomial matrix: computational aspects. *Linear Algebra Appl.*, 50:545–579, 1983.

[48] A. Amiraslani, R.M. Corless, and P. Lancaster. Linearization of matrix polynomials expressed in polynomial bases. *IMA. J. Number. Anal*, 1:141–157, 2009.

[49] P. Van Dooren. The computation of kronecker's canonical form of a singular pencil. *Linear Algebra and its Applications*, 27:103–140, 1979.

[50] Th. Beelen and P. Van Dooren. An improved algorithm for the computation of Kronecker's canonical form of a singular pencil. *Linear Algebra Appl.*, 105:9–65, 1988.

[51] B. Mourrain. Computing isolated polynomial roots by matrix methods. *J. of Symbolic Computation, Special Issue on Symbolic-Numeric Algebra for Polynomials*, 26(6):715–738, Dec. 1998.

[52] B. Mourrain. Bezoutian and quotient ring structure. *J. of Symbolic Computation*, 39(3):397–415, 2005.

[53] F. Chen, W. Wang, and Y. Liu. Computing singular points of plane rational curves. *J. Symbolic Comput*, 43(2):92–117, 2008.

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

[55] R. Rubio, J.M. Serradilla, and M.P.Vélez. Detecting real singularities of a space curve from a real rational parametrization. *Journal of Symbolic Computation*, 44:490–498, 2009.

[56] G. W. Stewart. On the sensitivity of the eigenvalue problems $ax = \lambda bx$. *SIAM J. Numer. Anal. 9*, 4:669–689, 1972.

[57] A. Mantzaflaris and B. Mourrain. A subdivision approach to planar semi -algebraic sets. In *Proceedings of the 6th international Conference GMP, Castro Urdiales, Spain*, pages 104–123, June 2010.

[58] M. Elkadi, A. Galligo, and T. Luu Ba. Approximate gcd of several univariate polynomials, small degree perturbations. *Journal of Symbolic Computation, issue in honour of Joachim von zur Gathen*, 2011.

[59] N. Howgrave-Graham. *Approximate integer common divisors*. In *Cryptography and lattices (Providence, RI, 2001)*. volume 2146 of *Lecture Notes in Comput. Sci.*, pages 51–66. Springer, Berlin, 2001.

[60] M. Van Dijk, C. Gentry, S. Halavi, and V. Vaikuntanathan. *Fully homomorphic encryption over the integers*. In *Advances in cryptology – EUROCRYPT 2010*, volume 6110 of *Lecture Notes in Computer Science*, pages 24–43. Springer, Berlin, 2010.

[61] D. A. Bini and P. Boito. Structured matrix-based methods for polynomial ϵ-gcd: analysis and comparisons. In *In ISSAC, ACM, New York*, pages 9–16, 2007.

[62] I. Z. Emiris, A. Galligo, and H. Lombardi. Certified approximate univariate GCDs. *J. Pure Appl. Algebra*, 117/118:229–251, 1997.

[63] E. Kaltofen, Z. Yang, and L. Zhi. Approximate greatest common divisors of several polynomials with linearly constrained coefficients and singular polynomials. In *In* ISSAC 2006*, ACM, New York*, pages 169–176, 2006.

[64] N. K. Karmarkar and Y. N. Lakshman. On approximate GCDs of univariate polynomials. *J. Symbolic Comput*, 26(6):653–666, 1998.

[65] V. Y. Pan. Computation of approximate polynomial GCDs and an extension. *Inform. and Comput*, 167(2):71–85, 2001.

[66] D. Rupprecht. An algorithm for computing certified approximate GCD of n univariate polynomials. *J. Pure Appl. Algebra*, 139(1-3):255–284, 1999.

[67] T. Sasaki and M.-T. Noda. Approximate square-free decomposition and root-finding of ill-conditioned algebraic equations. *J. Inform. Process*, 12(2):159–168, 1989.

[68] A. Galligo. *À propos du théorème de-préparation de Weierstrass*. In Fonctions de plusieurs variables complexes (Sém. François Norguet, octobre 1970–décembre 1973; à la mémoire d'André Martineau). Pages 543–579. Lecture Notes in Math., Vol. 409. Springer, Berlin, 1974.

[69] D. Bayer. *The division algorithm and the Hilbert scheme.* PhD thesis, Harvard University. 1982.

[70] D. Mumford. Algebraic Geometry I: Complex Projective Varieties*, volume 221 of* Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Springer-Verlag, Berlin, 1981.

[71] J. von zur Gathen and J. Gerhard. *Modern computer algebra*. second edition. Cambridge University Press, Cambridge, 2003.

[72] C. D'Andrea. On the structure of μ-classes. *Comm. Algebra*, 32(1):159–165, 2004.

Répresentation Matricielle Implicite de Courbes et Surfaces algébriques et Applications

Résumé. Dans cette thèse, nous introduisons et étudions une nouvelle représentation implicite des hypersurfaces rationelles et des courbes rationnelles plongées dans un espace projectif de dimension arbitraire. Nous illustrons les avantages de cette représentation matricielle en abordant plusieurs problèmes importants intervenant en conception géométrique assistée par ordinateur: les problèmes d'intersection entre deux courbes, entre une courbe et une surface ou bien encore entre deux surfaces, le problème d'appartenance d'un point à une courbe ou une surface, le problème du calcul de la pré-image d'un point donné par une paramétrisation et enfin le problème du calcul des singularités d'une courbe rationnelle. L'approche développée dans ce travail de thèse est basée sur la combinaison de méthodes symboliques et numériques. En effet, un première étape symbolique consiste à transformer le problème considérer en un pinceau de matrices. La deuxième étape consiste alors à calculer les valeurs propres généralisées de ce pinceau à l'aide de méthodes numériques. Pour cela, un algorithme d'extraction de la partie régulière d'un pinceau univarié, respectivement bivarié, de matrices non carrées est présenté. Une implémentation de ces travaux dans les systèmes de calcul formel *Mathemagix* et *Maple* est présentée en appendice. Le dernier chapitre est conscré à un algorithme qui, étant donné un ensemble de polynômes univariés $f_1, ..., f_s$ construit un ensemble de polynômes $u_1, ..., u_s$ dont les degrés sont prescrits, tels que le degré du pgcd$(f_1 + u_1, ..., f_s + u_s)$ est supérieur ou égal à un entier donné sous des hypothèses de généricité.

Mots-clés: μ-base, l'élimination, représentations matricielles, problèmes d'intersection, singularités, implicitation, pinceau de matrices, formes de Kronecker, idéal initial générique, PGCD de polynômes, suite normale des degrés, bases de Gröbner.

Matrix-based implicit representations of algebraic curves and surfaces and applications

Abstract. In this thesis, we introduce and study a new implicit representation of rational curves of arbitrary dimensions and propose an implicit representation of rational hypersurfaces. Then, we illustrate the advantages of this matrix representation by addressing several important problems of Computer Aided Geometric Design (CAGD): The curve/curve, curve/surface and surface/surface intersection problems, the point-on-curve and inversion problems, the computation of singularities of rational curves. We also develop some symbolic/numeric algorithms to manipulate these new representations for example: the algorithm for extracting the regular part of a non square pencil of univariate polynomial matrices and bivariate polynomial matrices. In the appendix of this thesis work we present an implementation of these methods in the computer algebra systems *Mathemagix* and *Maple*. In the last chapter, we describe an algorithm which, given a set of univariate polynomials $f_1, ..., f_s$ returns a set of polynomials $u_1, ..., u_s$ with prescribed degree-bounds such that the degree of $\gcd(f_1 + u_1, ..., f_s + u_s)$ is bounded below by a given degree assuming some genericity hypothesis.

Keywords: μ-basis, elimination, matrix representations, intersection problems, singularities, implicitation, pencils matrices, Kronecker form, generic initial ideal, GCD of univariate polynomials, normal degree sequence, Gröbner basis.