UNIVERSITÉ CÔTE D'AZUR

ÉCOLE DOCTORALE
SCIENCES FONDAMENTALES ET APPLIQUÉES

Représentations matricielles des fibres finies d'applications rationnelles et problèmes de distances

INRIA Sophia Antipolis Méditerranée, Équipe Aromath

Fatmanur YILDIRIM

Présentée en vue de l'obtention du grade de docteur en mathématiques
d'Université Côte d'Azur
Dirigée par Laurent Busé
Soutenue le 3 Février 2020

Devant le jury composé de:

M. Mohamed Barakat	Professor, Universität Siegen
Mme Alessandra Bernardi	Associate professor, Università Di Trento
M. Laurent Busé	Chargé de recherche, Université Côte d'Azur, Inria
Mme Julie Déserti	Maître de conférences, Université Côte d'Azur
M. Daniele Faenzi	Professeur des universités, Université de Bourgogne
M. André Galligo	Professeur émérite, Université Côte d'Azur
M. Bernard Mourrain	Directeur de recherche, Université Côte d'Azur, Inria
M. Juan Carlos Naranjo	Profesor titular de universidad, Universitat de Barcelona

Marie Skłodowska-Curie Actions

ARCADES

Inria INVENTEURS DU MONDE NUMÉRIQUE

Représentations matricielles des fibres finies d'applications rationnelles et problèmes de distances

Finite fibers of rational maps by means of matrix representations with applications to distance problem

Jury :

Rapporteurs :

Mme Alessandra Bernardi	Associate professor, Università Di Trento
M. Josef Schicho	Associate professor, Johannes Kepler Universität Linz

Examinateurs :

M. Mohamed Barakat	Professor, Universität Siegen
Mme Alessandra Bernardi	Associate professor, Università Di Trento
M. Laurent Busé	Chargé de recherche, Université Côte d'Azur, Inria
Mme Julie Déserti	Maître de conférences, Université Côte d'Azur
M. Daniele Faenzi	Professeur des universités, Université de Bourgogne
M. André Galligo	Professeur émérite, Université Côte d'Azur
M. Bernard Mourrain	Directeur de recherche, Université Côte d'Azur, Inria
M. Juan Carlos Naranjo	Profesor titular de universidad, Universitat de Barcelona

Abstract

In this thesis, implicit matrix-based representations of finite fibers of rational maps are studied theoretically and computationally for two problems: implicitization of rational algebraic curves in arbitrary dimension and orthogonal projections of a point onto an rational algebraic surface in three dimensional space. The proposed matrices have the property that their cokernels at a given point p in the target space of the rational map are in relation with the pre-images of the p via this rational map. In addition, these matrices can be pre-computed so that the pre-images of such a point p can be approximately computed by means of fast and robust numerical linear algebra tools.

In the second chapter, a new family of implicit matrix representations is introduced for algebraic curves. It relies on the use of moving quadrics following curve parameterizations and provides a high-order extension of the implicit matrix representations built from their linear counterparts, the moving planes. Such matrices offer new, more compact, implicit representations of rational curves. Their entries are filled by linear and quadratic forms in the space variables and their ranks drop exactly on the curve. Typically, for a general rational curve of degree d we obtain a matrix whose size is half of the size of the corresponding matrix obtained with the moving planes method.

In the third chapter, the problem of computing the orthogonal projections of a point onto a rational algebraic surface embedded in three dimensional projective space is turned into the problem of computing the finite fibers of a generically finite dominant rational map: a congruence of normal lines to the rational surface. Then, an in-depth study of certain syzygy modules associated to such a congruence is presented and applied to build elimination matrices that provide universal representations of its finite fibers, under some genericity assumptions. Moreover, these matrices depend linearly in the variables of the three dimensional space and can be pre-computed for a given rational surface.

Lastly, the appendix of this thesis reports on a three-month industrial secondment at the company Missler Software where two distance problems are treated : distance between a circle and a line in 3D and distance between an arc of a circle and a segment of a line in three dimensional space.

Key words : multi-graded rational map, implicitization, parameterization, fiber, distance, orthogonal projection, syzygies, μ-basis, moving quadric.

Résumé

Dans cette thèse, de nouvelles représentations matricielles des fibres finies d'applications rationnelles sont introduites et étudiées d'un point de vue théorique mais aussi pratique avec l'objectif de traiter des problèmes de distances, notamment les deux problèmes suivant: l'implicitation des courbes rationnnelles algébriques en dimension arbitraire et la détermination des projetés orthogonaux d'un point sur une surface rationnelle algébrique en dimension trois. Les noyaux à gauche de ces représentations matrices, après évaluation en un point p de l'espace ambiant sont reliés aux pré-images du point p par l'application rationnelle considérée. De plus, ces matrices peuvent être pré-calculées et les pré-images d'un point p peuvent être calculées approximativement de manière efficace et robuste grâce aux outils d'algèbre linéaire.

Dans le deuxième chapitre, une nouvelle famille des représentations matricielles est proposée pour les courbes algébriques rationnelles. Elle est basée sur le concept de 'quadriques mobiles' associées aux courbes parametrées. Elle fournit une extension non linéaire des représentations matricielles qui sont obtenues au moyen du concept plus classique de 'plans mobiles' associés à une paramétrisation. Ces matrices fournissent ainsi de nouvelles représentations implicites plus compactes pour les courbes rationnelles algébriques. Leurs entrées sont composées de formes linéaires et quadratiques en les variables de l'espace ambiant et leur rang chute exactement sur la courbe considérée. De plus, pour une courbe rationnelle générale de degré d ces nouvelles matrices sont deux fois plus petites en taille que les matrices, plus classiques, qui n'utilisent que des plans mobiles, et donc dont les entrées sont exclusivement composées de formes linéaires.

Dans le troisième chapitre, le calcul des projetés orthogonaux d'un point sur une surface rationnelle algébrique dans l'espace projectif de dimension trois est étudié comme un problème d'inversion, plus précisément comme le calcul des fibre finies d'applications rationnelles génériquement finies et dominantes : les congruences des droites normales à une surface algébrique rationnelle. Une analyse fine des modules de relations (syzygies) associés à ces congruences est tout d'abord menée, puis utilisée pour construire des matrices eliminantes qui fournissent des représentations universelles de ces fibres finies. De plus, ces matrices dépendent linéairement des variables de l'espace ambiant de dimension trois et elles peuvent être pré-calculées pour une surface algébrique rationnelle donnée.

Enfin, l'appendice de cette thèse décrit les résultats obtenus lors d'un séjour de recherche mené chez le partenaire industriel Missler Software. Deux problèmes de distance en dimension trois ont été étudiés: le calcul de la distance entre un cercle et une droite puis le calcul de la distance entre un arc de cercle et un segment de droite.

Mots-clés : application rationnelle multi-graduée, implicitisation, paramétrisation, fibre, distance, projection orthogonale, syzygies, μ-base, quadriques mobiles.

Remerciements

Avant tout, je tiens à remercier chaque membre de l'équipe Aromath à l'Inria Sophia Antipolis et également à l'Athena à Athènes. Je remercie également Alessandra Bernardi et Josef Schicho qui ont accepté d'être rapporteurs de cette thèse.

Je tiens à remercier mon directeur de thèse, Laurent Busé, pour sa disponibilité, sa patience, sa compréhension, ses conseils, et son aide qui m'a permis d'acquérir des connaissance en algèbre commutative et géometrie algébrique pendant trois ans. Je tiens à remercier Marc Chardin pour avoir accepté de venir à Nice plusieurs fois, pour nos discussion pendant des heures et aussi pour m'avoir aidée repousser toujours plus loin les limistes de mes connaissances. Je remercie à Bernard Mourrain pour nos discussions encourageantes de tous les jours pendant le déjeuner.

Je remercie aussi d'abord Carlos D'Andrea pour sa supervision pendant ma visite de trois mois à l'Université de Barcelone et nos discussions, ensuite Santiago Zarzuela et Casas Alvero pour ses cours que j'ai suivis et pour m'avoir encouragée de donner ma première présentation.

Je remercie aussi d'abord Christian Arber pour m'avoir accepté de faire une visite de 3 mois chez Missler Software à Toulouse où j'ai eu une expérience dans l'industrie pour la première fois. Je remercie aussi chaque membre de l'équipe projet Européen de Missler Software, pour son accueillance, son disponibilité, pour m'avoir aidée avancer rapidement. Je remercie évidemment à mon encadrant chez Missler Software, Frédéric Vidil, pour sa disponibilité et pour sa tranquilité qui m'a beaucoup appris de comment il faut coder.

Je tiens à remercier tous mes amis, les nouveaux amis que j'ai rencontrés pendant ma thèse, tous ESR d'ARCADES qui m'ont donné leurs soutiens et leurs temps pendant tout au long de mon doctorat.

Son olarak, tüm aileme ve arkadaşlarıma destekleri, hoş sohbetleri ve tüm paylaştıklarımız için teşekkür ederim.

Acknowledgement

My research was funded by the project ARCADES which has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 675789.

Cette thèse est dédiée d'abord à mon père Yılmaz Yalçın et ma mère Nurten ensuite à tous ceux qui sont comme ma famille.

Bu tez babam Yılmaz Yalçın, annem Nurtiş'ime ve bana aile olan herkese adanmıştır.

Contents

Introduction

Rational maps are fundamental objects in algebraic geometry. In the field of Computer-Aided Geometric Design (CAGD) and geometric modeling, they are used to describe geometric objects. For instance, the image of rational maps are used to give parametric representations of geometric objects as *parameterizations of for example curves and surfaces*. To illustrate, the unit sphere in $\mathbb{R}^3$ is usually parameterized by the rational map ϕ

$$\begin{array}{rccc} \phi: & \mathbb{A}^2_{\mathbb{R}} & \to & \mathbb{A}^3_{\mathbb{R}} \\ & (u,v) & \mapsto & \left(\frac{2u}{1+u^2+v^2}, \frac{2v}{1+u^2+v^2}, \frac{-1+u^2+v^2}{1+u^2+v^2}\right). \end{array}$$

Parametric algebraic curves and surfaces can be also described by *implicit representations* as the set of points verifying common zeros of polynomial equation(s). To illustrate, we consider again the unit sphere in $\mathbb{R}^3$. Then, the zeros of the equation

$$x^2 + y^2 + z^2 - 1 = 0 \text{ where } (x, y, z) \in \mathbb{R}^3$$

define the unit sphere in $\mathbb{R}^3$, i.e. $x^2 + y^2 + z^2 - 1 = 0$ is its implicit equation. Here, we emphasize that only one polynomial equation is enough to represent implicitly a plane curve, whereas we need several polynomial equations for curves and surfaces in space over $\mathbb{C}$. Both representations are intensively used in Computer-Aided Geometric Design (CAGD) and geometric modeling depending on the problem. Nevertheless, we emphasize that the implicit equation(s) of a given parametric geometric object looses information about parameter values.

Very interesting and useful knowledge about a given geometric object in geometric modeling is how many distinct parameter values correspond to the same point p on the given object, and what their coordinates are. Indeed, in CAGD, instead of the entire geometric object, generally a patch of it is considered. Equivalently we consider its parameterization only in some intervals of parameter values. The investigation of which parameter values of p are on the patch requires more information than what the implicit equations provide. Seeking for answers to these questions leads to study the *fibers of the corresponding parameterization, i.e. rational map.*

Let k be a field and Φ be a rational map from $\mathbb{P}^n_k$ to $\mathbb{P}^m_k$ given by homogeneous polynomials $F_0, \ldots, F_m$ of degree d in the coordinate ring $R = k[x_0, \ldots, x_n]$. Then, the closed image of Φ is a subvariety in $\mathbb{P}^m_k$. Moreover, from the graph Γ_Φ of the rational map Φ, we have two canonical projections, the first one is on the first component, i.e. $\pi_1 : \Gamma_\Phi \to \mathbb{P}^n_k$, the second one is on the last component, i.e. $\pi_2 : \Gamma_\Phi \to \mathbb{P}^m_k$.

$$\begin{array}{ccc} \Gamma_\Phi & \hookrightarrow & \mathbb{P}^n_k \times \mathbb{P}^m_k \\ {\scriptstyle \pi_1}\downarrow & \swarrow_{\pi_2} & \\ \mathbb{P}^n_k & \overset{\Phi}{\dashrightarrow} & \mathbb{P}^m_k. \end{array}$$

Then, the closed image of Φ is the image of π_2. We define the *fiber over the point* p in $\mathbb{P}^m_k$ as the pre-images along π_2 of p and we denote it as $\pi_2(p)^{-1}$.

Moreover, the investigation of whether the fiber is empty answers the *implicitization* problem. *The first part of my thesis studies the fibers of rational maps from* $\mathbb{P}^1_k$ *to* $\mathbb{P}^m_k$*, for any integer* $m \geqslant 2$ *by means of implicit matrices built from both linear (syzygies) and quadratic relations between the coordinates of* Φ *for the rational algebraic curve implicitization problem.*

We can describe a rational algebraic surface $\mathcal{S}$ as used in CAGD by a parameterization of the form $\Phi : X \dashrightarrow \mathbb{P}^3_k$, where X is either $\mathbb{P}^1_k \times \mathbb{P}^1_k$ (rational tensor-product surface) or $\mathbb{P}^2_k$ (rational triangular surface). Let $k[\underline{x}]$ be the coordinate ring of X. We know that in Euclidean geometry the orthogonal projections of a point p onto the surface $\mathcal{S}$ in $\mathbb{P}^3_k$ lie on the normal lines to the surface $\mathcal{S}$ passing through the point p. With the goal to compute the orthogonal projections of p onto $\mathcal{S}$, we study the fiber over p of the *multi-graded dense rational map* Ψ, which is a parameterization of the normal lines of the surface $\mathcal{S}$. We assume that the fiber over p is finite, i.e. there are finitely many orthogonal projections onto $\mathcal{S}$. The rational map Ψ is of form $\Psi : X \times \mathbb{P}^1_k \to \mathbb{P}^3_k$ such that $\Psi(\underline{x}) = \bar{t}\Phi(\underline{x}) + t\nabla(\underline{x})$, where $\nabla(\underline{x})$ is the homogeneous normal vector to $\mathcal{S}$ (see §3.1.3 for the details) and $k[\bar{t}, t]$ is the coordinate ring of the last $\mathbb{P}^1_k$. It is of degree $(\boldsymbol{d}, 1)$ on $X \times \mathbb{P}^1_k$ where $\boldsymbol{d}$ is bidegree if $X = \mathbb{P}^1_k \times \mathbb{P}^1_k$ or $\boldsymbol{d}$ is degree if $X = \mathbb{P}^2_k$. Moreover, for a general rational surface we observe that the base locus of the rational map Ψ, i.e. points in $X \times \mathbb{P}^1_k$ where Ψ_0, Ψ_1, Ψ_2 and Ψ_3 vanish simultaneously is of *dimension one* (see Lemma 3.1.2). Once, we know the orthogonal projections of p onto $\mathcal{S}$, then we can compute the distance between the point p and the surface $\mathcal{S}$ which will be the smallest among the distances between p and its orthogonal projections. *In a second part, my thesis studies the finite fibers of multi-graded rational dominant maps onto three dimensional projective space and its application to the computation of orthogonal projections of a point onto a rational algebraic surface.*

Finally, in the last chapter, my thesis reports on *3-month industrial secondment in Missler Software in France where I treated distance between a circle and a line and also between an arc of a circle and a line segment in space.*

Curve implicitization

In what follows, we give a short overview about existing works on the implicitization of plane curves and introduce the contribution of this thesis on this topic. Let $\Phi : \mathbb{P}^1_k \to \mathbb{P}^2_k$ be a parameterization of a plane curve $\mathcal{C}$ given by

$$(s : t) \mapsto (F_0(s,t) : F_1(s,t) : F_2(s,t)),$$

where F_0, F_1, F_2 are homogeneous polynomials of the same degree $d \geqslant 1$ in $k[s,t]$. Implicit representations are particularly interesting for determining whether a point lies on the curve $\mathcal{C}$, also for solving curve/curve intersection problems. Therefore, the implicitization of rational plane curves have been extensively studied for those reasons in CAGD. One main approach is to use the *resultant*. Let $k[T_0, T_1, T_2]$ be the coordinate ring of $\mathbb{P}^2_k$. Consider the polynomials

$$\begin{aligned} F_0T_1 - F_1T_0 &= a_0(T_0,T_1,T_2)t^d + a_1(T_0,T_1,T_2)st^{d-1} + \cdots + a_d(T_0,T_1,T_2)s^d \quad \text{and} \\ F_0T_2 - F_2T_0 &= b_0(T_0,T_1,T_2)t^d + b_1(T_0,T_1,T_2)st^{d-1} + \cdots + b_d(T_0,T_1,T_2)s^d. \end{aligned}$$

Then, the classical *Sylvester matrix* of $F_0T_1 - F_1T_0$ and $F_0T_2 - F_2T_0$

$$\mathrm{Syl}(F_0T_1 - F_1T_0, F_0T_2 - F_2T_0) = \begin{bmatrix} a_d & & & b_d & & \\ a_{d-1} & \ddots & & b_{d-1} & \ddots & \\ \vdots & \ddots & a_d & \vdots & \ddots & b_d \\ \vdots & & a_{d-1} & \vdots & & b_{d-1} \\ a_0 & & \vdots & b_0 & & \vdots \\ & \ddots & \vdots & & \ddots & \\ & & a_0 & & & b_0 \end{bmatrix}$$

is a $2d \times 2d$ matrix with linear entries in T_0, T_1, T_2 and of which determinant is given by

$$\mathrm{Res}(F_0T_1 - F_1T_0, F_0T_2 - F_2T_0) = T_0^d C(T_0, T_1, T_2)^{\deg(\Phi)},$$

where $C(T_0, T_1, T_2)$ is the implicit equation of the curve (defined up to a nonzero constant factor) and $\deg(\Phi)$ is the degree of the map Φ. When k is algebraically closed, then $\deg(\Phi)$ is the number of pre-images of a generic point on the curve $\mathcal{C}$ via Φ.

There exist also the methods based on *moving lines* for the implicitization problem. The moving lines have been introduced by Sederberg and Chen in [73]. A moving line L is a polynomial

$$L(T_0, T_1, T_2; s, t) := A(s,t)T_0 + B(s,t)T_1 + C(s,t)T_2.$$

For fixed s, t values, the equation $L = 0$ defines a line that moves when the parameter value s, t of the curve moves. We say that the moving line L follows the rational plane curve $\mathcal{C}$ if

$$L(\Phi(s,t); s, t) = A(s,t)F_0(s,t) + B(s,t)F_1(s,t) + C(s,t)F_2(s,t) = 0.$$

Let $I := (F_0, F_1, F_2)$ be the ideal of $k[s,t]$. *The syzygy module of the ideal* I is defined as

$$\mathrm{Syz}(I) := \{(g_0, g_1, g_2) \in k[s,t]^3 : g_0F_0 + g_1F_1 + g_2F_2 = 0\}.$$

Thus, $(A(s,t), B(s,t), C(s,t))$ is a syzygy of I if L follows Φ. Moreover it is known that $\mathrm{Syz}(F_0, F_1, F_2)$ is a free $k[s,t]$-module of rank 2 (see [31]). We denote a couple of generators by $p := (p_0, p_1, p_2)$ and $q := (q_0, q_1, q_2)$. The couple p, q is called a *μ-basis* (see [31]). Let $\deg(p) = \mu_1, \deg(q) = \mu_2$ and $\mu_1 \leqslant \mu_2$. The μ-basis p, q verifies $\mu_1 + \mu_2 = d$. It is known that for a general plane curve of degree d, we have $\mu_2 = \lceil \frac{d}{2} \rceil$ (see [31]).

There are several existing works on μ-basis. In [31], the method of moving lines following a given plane curve is studied with μ-basis notion. Later in [26], more properties and equivalent definitions of a μ-basis of I for a rational plane curve are given in terms of moving line method with an algorithm based on Gaussian elimination computing the μ-basis. In [73], matrix of moving lines is interpreted as the Sylvester matrix of μ-basis of I, denoted by $\mathrm{Syl}(p, q)$. $\mathrm{Syl}(p, q)$ is of size $d \times d$ of which determinant yields a polynomial of degree d in $k[T_0, T_1, T_2]$. We remark that the matrix $\mathrm{Syl}(p, q)$ has half size of the matrix $\mathrm{Syl}(F_0T_1 - F_1T_0, F_0T_2 - F_2T_0)$, which implies that the use of μ-basis allows us to decrease the size of the implicit matrix whose determinant yields the implicit equation of $\mathcal{C}$. Moreover, the matrix $\mathrm{Syl}(p, q)$, without computing its determinant, can be used for determining if a point lies on

the curve simply by evaluating its rank at this point. Then its parameter(s) can be determined from the kernel of this matrix, whereas this is not possible to do with an implicit polynomial equation of the curve $\mathcal{C}$. For that reason, *instead of dealing with the polynomials of higher degree obtained by such determinants, the developed results in this thesis focus on the matrix itself as an implicit representation of the curve* $\mathcal{C}$.

In Chapter 2, we consider Hybrid Bézout matrices of μ-basis that we denoted by $\mathbb{MQ}$. Let p and q be as follows,

$$p = a_0(T_0, T_1, T_2)t^{\mu_1} + a_1(T_0, T_1, T_2)st^{\mu_1-1} + \cdots + a_{\mu_1}(T_0, T_1, T_2)s^{\mu_1},$$

$$q = b_0(T_0, T_1, T_2)t^{\mu_2} + b_1(T_0, T_1, T_2)st^{\mu_2-1} + \cdots + b_{\mu_2}(T_0, T_1, T_2)s^{\mu_2}.$$

For plane curves, $\mathbb{MQ}$ is $\mu_2 \times \mu_2$ matrix which is composed by the last $\mu_2 - \mu_1$ columns of $\mathrm{Syl}(p, q)$ in coefficients of q and the first μ_1 columns of Bézout matrix of p and q. We recall that the Bézout matrix of p, q, denoted by $\mathrm{Bez}(p, q)$ is defined by $\mathrm{Bez}(p, q) = (b_{ij})_{1\leqslant i,j\leqslant d}$ where

$$\frac{p(\sigma,\tau)q(s,t) - p(s,t)q(\sigma,\tau)}{s\tau - t\sigma} = \sum_{1\leqslant i,j\leqslant d} b_{ij}t^{i-1}s^{d-i+1}\tau^{j-1}\sigma^{d-j+1},$$

and σ, τ are new indeterminates. Since $\mathrm{Bez}(p, q)$ has quadratic entries in T_0, T_1, T_2, Hybrid Bézout matrix consists of both linear and quadratic terms and its determinant yields a homogeneous polynomial of degree $(\mu_2 - \mu_1) + 2\mu_1 = d$ in T_0, T_1, T_2. This approach for obtaining such more compact implicitization matrices with some quadratic entries is also known as the method of moving conics (see [29]). A *moving conic* of degree ν in $\mathbb{N}$ is a polynomial of the form

$$\begin{aligned} Q(T_0, T_1, T_2; s, t) = {} & g_{0,0}(s, t)T_0^2 + g_{0,1}(s, t)T_0T_1 + \\ & g_{0,2}(s, t)T_0T_2 + g_{1,1}(s, t)T_1^2 + g_{1,2}(s, t)T_1T_2 + g_{2,2}(s, t)T_2^2 \end{aligned}$$

where the polynomials $g_{i,j}(s, t)$ are homogeneous polynomials of degree ν in $k[s, t]$. In addition, this moving conic is said to follow the parameterization ϕ if

$$Q(\Phi(s, t); s, t) = \sum_{0\leqslant i\leqslant j\leqslant 2} g_{i,j}(s, t)F_i(s, t)F_j(s, t) = 0.$$

Similarly to moving lines, this latter condition means geometrically that the conic Q goes through the point $\phi(s : t) \in \mathcal{C}$. The moving conics have been introduced in [74] and then extensively used, especially to deal with the implicitization of rational surfaces (see [61, 29]).

Unlike the case of plane curves, the implicitization of parameterized curves in higher dimension is much more delicate because now a space curve is not given by a single equation over algebraically closed field. Nevertheless, the concept of μ-basis is easily generalized to curves in higher dimension [52, 77] and from them many results to produce some implicit polynomial equations of a curve have been proposed. For instance [16] and [18] consist in using the elimination matrix built from a μ-basis as an implicit representation. Thus, this matrix of moving hyperplanes denoted by $\mathbb{M}$ is the natural generalization of the Sylvester matrix of a μ-basis in the case of plane curves. Although this matrix is no longer a square matrix, it still allows to characterize the point that lie on the curve by a drop of its rank. In [16], the construction and the properties of the matrix of moving hyperplanes $\mathbb{M}_\nu$ has been studied. Briefly, the

matrix $\mathbb{M}_\nu$ is filled by the syzygies of the ideal generated by the coordinates of a parameterization of the space curve of a suitable degree ν. We will say that $\mathbb{M}_\nu$ is the matrix of moving hyperplanes at given degree ν. Some applications such that inversion of a point on a curve by means of generalized eigenvalues computation, multiplicity of a point p on a curve by means of drop of rank of $\mathbb{M}_\nu$ evaluated at p are explained in details. Furthermore, intersection problems are studied. More precisely, intersection of two curves is studied by substituting the parameterization of the first curve $\mathcal{C}_1$ into a suitable implicit matrix $\mathbb{M}_\nu$ of the second curve $\mathcal{C}_2$. Then, one may consider the two companion matrices of the cokernel of $\mathbb{M}_\nu$, then reduce them into two square full rank matrices by Kronecker form (see [63, §3.2], [16, §6.2.]), and after that compute their generalized eigenvalues in order to compute the coordinates of the intersection points. Similar matrices are also used for curve/surface, surface/surface intersection problems (see [17, 63]).

From now on, let Φ be the parameterization

$$\begin{array}{rccl} \Phi: & \mathbb{P}^1_k & \to & \mathbb{P}^m_k \\ & (s:t) & \mapsto & (F_0(s,t):F_1(s,t):\ldots:F_m(s,t)) \end{array}$$

where $F_0,\ldots,F_m$ are homogeneous polynomials of degree $d \geqslant 1$ in $k[s,t]$. Let $I := (F_0,\ldots,F_m)$ be an ideal of $k[s,t]$. Then, the μ-basis notion can be generalized to higher dimensions $m \geqslant 2$ for curves, since the syzygy module of I, denoted by $\mathrm{Syz}(I)$, is still free and $\mathrm{Syz}(I)$ is generated by m vectors of homogeneous polynomials, whose degrees sum up to d, according to Hilbert-Burch Theorem (see [9]). We will still assume that $\mu_1 \leqslant \cdots \leqslant \mu_m$, where μ_i's are the degrees of μ-basis. We refer the reader to the work [77] which generalizes moving line methods in [26] into higher dimensions, i.e. generalizes to the rational space curves in arbitrary dimension. In addition, [51] gives explicitly the properties of μ-basis of space curve parameterization Φ with an algorithm based on partial reduced row-echelon form of a coefficient matrix of Sylvester type which is faster than the previous known methods in [77, 26].

Back to the use of resultant type matrices for implicitization problem, in Chapter 2 we generalize the Hybrid Bézout matrix of μ-basis into higher dimensions. We construct it by concatenating the matrix of moving hyperplanes and matrix of moving quadrics at given degree ν and denote it by $\mathbb{MQ}$. We also show the strong relation between the matrices $\mathbb{MQ}$ and degree of the fiber over a point p on the given curve $\mathcal{C}$.

We first recall that for all R-module M where R is a graded ring and $k = R_0$ is a field, we define *Hilbert function of* M as

$$HF_M(\mu) = \dim_k(M_\mu),$$

and *Hilbert series of* M as

$$HS_M(x) = \frac{L_M(x)}{(1-x)^\delta},$$

where δ denotes the Krull dimension of M and $L_M(x)$ is the unique polynomial verifying $L_M(a) \neq 0$ (see [41, §1.9], [9, Chapter 4]). We define *Hilbert polynomial of* M as

$$HP_M(\mu) = \frac{a_{\delta-1}}{(\delta-1)!}x^{\delta-1} + \cdots + a_0,$$

where $a_{\delta-1} = L_M(1)$. We also know that for all sufficiently large μ, Hilbert function is equal to Hilbert polynomial. Let p be a point in $\mathbb{P}^m_k$ having finite fiber $\pi_2^{-1}(p)$.

Then, for the μ degrees where the Hilbert function of $\pi_2^{-1}(p)$ is equal to the Hilbert polynomial of $\pi_2^{-1}(p)$, it is also equal to the degree of $\pi_2^{-1}(p)$.

Main result 1.(Theorem 2.2.1) Assume that $\nu \geqslant \mu_m - 1$. Let r_ν be the dimension of the vector space of moving hyperplanes in degree ν. Let c_ν be the dimension of the quotient vector space obtained as the vector space of moving quadrics modulo the vector space of moving hyperplanes, both in degree ν. Then, $r_\nu + c_\nu \geqslant \nu + 1$ and the degree of the fiber at $p \in \mathcal{C}$ is equal to corank of $\mathbb{MQ}_\nu(p)$. In particular,

$$\operatorname{rank}(\mathbb{MQ}_\nu(p)) < \nu + 1 \iff p \in \mathcal{C}.$$

Moreover, we have that

$$c_\nu = \sum_{1 \leqslant i < j \leqslant m} \max(0, \mu_i + \mu_j - 1 - \nu).$$

Also, if $\nu \geqslant \mu_m + \mu_{m-1} - 1$ then $c_\nu = 0$ and it follows that $\mathbb{MQ}_\nu = \mathbb{M}_\nu$.

After that, the structure of Hybrid Bézout is explained. Its quadratic relations are computed by Sylvester forms of μ-basis $p_1, \ldots, p_m$ of the parameterization Φ in §2.2.1. Let's first define *Sylvester forms*. Let $k[T_0, \ldots, T_m]$ be the coordinate ring of $\mathbb{P}_k^m$. Let $\mu_i \leqslant \mu_j$ be degrees of p_i and p_j. Let $\alpha := (\alpha_i, \alpha_j)$ be any couple of non-negative integers such that $|\alpha| := \alpha_i + \alpha_j \leqslant \mu_i - 1$. Since p_i and p_j are homogeneous polynomials in the variables s, t, one can decompose them as

$$\begin{aligned} p_i &= s^{\alpha_i+1} h_{i,1} + t^{\alpha_j+1} h_{i,2}, \\ p_j &= s^{\alpha_i+1} h_{j,1} + t^{\alpha_j+1} h_{j,2}, \end{aligned}$$

where $h_{k,h}(s, t; T_0, \ldots, T_m)$ are homogeneous polynomials of degree $\mu_k - \alpha_h - 1$ with respect to the variables s, t and linear forms with respect to the variables $T_0, \ldots, T_m$. Then, we define the polynomial

$$\operatorname{syl}_\alpha(p_i, p_j) := \det \begin{pmatrix} h_{i,1} & h_{i,2} \\ h_{j,1} & h_{j,2} \end{pmatrix}$$

and call it a *Sylvester form* of p_i and p_j. Then, for any integer ν consider the vector space S_ν that is generated by all the Sylvester forms of degree ν, i.e.

$$\mathrm{S}_\nu = \langle \operatorname{syl}_\alpha(p_i, p_j) \text{ such that } \ 1 \leq i < j \leq m \text{ and } |\alpha| = \mu_i + \mu_j - 2 - \nu \rangle .$$

Main result 2.(Theorem 2.2.2) If $\nu \geq \mu_m - 1$, then the moving quadrics of degree ν following Φ are generated by the moving hyperplanes of degree ν following Φ and by the Sylvester forms of degree ν. Moreover, these latter Sylvester forms are linearly independent and hence

$$\dim(\mathrm{S}_\nu) = c_\nu = \sum_{1 \leqslant i < j \leqslant m} \max(0, \mu_i + \mu_j - \nu - 1).$$

Fibers of rational maps in dimension three

In what follows, a new method to study fibers of multi-graded rational dominant maps onto three dimensional space is presented. We start by mentioning some related works on fibers of rational maps emphasizing their assumptions on base locus before explaining our results that will be described in Chapter 3.

There exist many related works on properties of rational maps for instance their degrees (see [4, 36, 14, 43]), dimensions, and Jacobian matrices (see [25, 72]), birationality criteria (see [37, 72]), also on equations of Rees algebra of the ideal generated by the coordinates of the rational maps ([58, 59, 19, 59, 79]). We notice that mostly all these works assume that the base locus of the rational map is either empty or zero-dimensional (consists of finite number of isolated points).

In [2], degree and dimension of the fibers of a birational map $\Phi : X \dashrightarrow \mathbb{P}^3_k$ where X is either $\mathbb{P}^2_k$ or $\mathbb{P}^1_k \times \mathbb{P}^1_k$ (or more generally a toric variety), under assumption that *the base locus $\mathcal{B}$ of the rational map Φ consists of finitely many points and $\mathcal{B}$ is locally a complete intersection*, are studied in terms of singular matrices $\mathbb{M}$ based on some syzygies of Φ. The degree of the fiber over the point p in $\mathbb{P}^3_k$ is given in terms of corank of $\mathbb{M}$ evaluated at p.

In [25], the fibers of rational maps $\Phi : \mathbb{P}^n_k \dashrightarrow \mathbb{P}^m_k$ where Φ is generically finite onto its image are studied. It is shown that the number of $(n-1)$-dimensional fibers of such rational map Φ is bounded linearly in terms of the degree of the polynomials defining Φ. The result is obtained by studying the ideals of minors of the Jacobian matrix of Φ. In this approach, Φ is assumed to have *(possibly empty) base locus $\mathcal{B}$ containing finitely many points, which is not necessarily locally a complete intersection*. Moreover, Φ is assumed to be generically finite onto its image.

Later in [5], the multi-graded rational maps $\Phi : \prod_{1\leqslant i\leqslant s} \mathbb{P}^{r_i}_k \dashrightarrow \mathbb{P}^m_k$ with $m = 1 + \sum_{1\leqslant i\leqslant s} r_i$ and *finite base locus* are studied for the implicitization of rational multi-projective hypersurfaces.

As far as we know the rational maps having *base locus of dimension one* were treated for the first and only time in [23] for the problem of hypersurface implicitization, i.e. for computing the equation of the closed image of for instance the map $\Phi : \mathbb{P}^{m-1}_k \dashrightarrow \mathbb{P}^m_k$.

In Chapter 3, we study the finite fibers of multi-graded, dense, rational maps $\Psi : X \times \mathbb{P}^1_k \dashrightarrow \mathbb{P}^3_k$, where X is either $\mathbb{P}^1_k \times \mathbb{P}^1_k$ or $\mathbb{P}^2_k$. Such a map Ψ is defined by the homogeneous polynomials $\Psi_0, \Psi_1, \Psi_2, \Psi_3$ of the same degree $(\boldsymbol{d}, e)$ over homogeneous coordinate ring $R := k[\underline{x}, t, \overline{t}] = k[\underline{x}] \otimes_k k[t, \overline{t}] = R_X \otimes R_1$ with k is a field and $\underline{x} = (x_0, \ldots)$, $R_X = k[\underline{x}]$ and $R_1 = k[t, \overline{t}]$ are the coordinate ring of X and $\mathbb{P}^1_k$ respectively. Hence, $(\boldsymbol{d}, e)$ is the degree on $X \times \mathbb{P}^1_k$. The main difficulty that we deal with in Chapter 3 is coming from our assumption that Ψ has a *one dimensional base locus $\mathcal{B}$*, i.e. the variety on which the coordinates of Ψ vanish has at most one-dimensional component. This latter requirement is the most technical property that is treated in this thesis.

Our contribution is more general. More precisely we consider any such rational map Ψ of degree $(\boldsymbol{d}, e)$ from $X \times \mathbb{P}^1_k$ to $\mathbb{P}^3_k$. Since the fibers of the rational map Ψ are not well defined, we need to consider its graph. The defining equations of this graph are known to be the equations of the multi-graded Rees algebra of the ideal I generated by the coordinates of Ψ, that we denote by $\mathrm{Rees}(I)$.

We recall that *Rees algebra* of the ideal $I := (\Psi_0, \Psi_1, \Psi_2, \Psi_3)$ with respect to the ring R is

$$\mathrm{Rees}(I) := \oplus_{i\geqslant 0} I^i z^i \subset R[z].$$

The Rees algebra $\mathrm{Rees}(I)$ inherits the multi-grading via the natural map

$$\begin{array}{rccc} \alpha : & R[T_0, T_1, T_2, T_3] & \to & \mathrm{Rees}(I) \subset R[z] \\ & T_i & \mapsto & \Psi_i z. \end{array}$$

It is known that it is difficult to compute the equations of Rees algebra, for this reason we approximate Rees algebra by symmetric algebra. We refer the reader to [80, 48, 50] for further details about Rees algebra.

Let's denote the ring $R[T_0, T_1, T_2, T_3]$ by S and the ring $k[T_0, T_1, T_2, T_3]$ by R'. Let $\ker(\alpha) = \mathfrak{p}$ an homogeneous ideal of S. We set $\mathfrak{p}_{(\boldsymbol{\mu},\nu)} \subset R_{\boldsymbol{\mu}} \otimes_k R'_\nu$, namely $\boldsymbol{\mu}$ is degree over $X \times \mathbb{P}^1_k$ and ν is degree over $\mathbb{P}^3_k$. We have the S-ideal generated by the syzygies of the ideal $I := (\Psi_0, \ldots, \Psi_3)$, i.e.

$$(\mathfrak{p}_{(*,1)}) = (\{\sum_{i=0}^{3} g_i T_i : g_i \in R \text{ and } \sum_{i=0}^{3} g_i \Psi_i = 0\}).$$

Moreover, we have the following surjective maps

$$S \to S/(\mathfrak{p}_{(*,1)}) \simeq \mathrm{Sym}(I) \text{ and } \mathrm{Sym}(I) \to \mathrm{Rees}(I) \simeq S/(\mathfrak{p}),$$

where $\mathrm{Sym}(I)$ is called the *symmetric algebra* of the ideal I. Consider the graph Γ_Ψ of Ψ:

$$\begin{array}{ccc} \Gamma_\Psi & \hookrightarrow & X \times \mathbb{P}^3_k \\ \downarrow{\scriptstyle \pi_1} & \swarrow{\scriptstyle \pi_2} & \\ X & \overset{\Phi}{\dashrightarrow} & \mathbb{P}^3_k \end{array}$$

We define the fiber over the point $p \in \mathbb{P}^3_k$ as the pre-images along π_2 of p, i.e. $\pi_2(p)^{-1}$. In particular, the fiber over p is a subscheme $\mathfrak{F}_p = \mathrm{Proj}(\mathrm{Rees}(I) \otimes \kappa(p)) \subset X \times \mathbb{P}^1_k$, where $\kappa(p)$ is the residue field of p. We consider symmetric algebra of the ideal I, more precisely the subscheme $\mathfrak{L}_p = \mathrm{Proj}(\mathrm{Sym}(I) \otimes \kappa(p))$ of $X \times \mathbb{P}^1_k$. We call $\mathfrak{L}_p$ as the *linear fiber of* p. We notice that the fiber $\mathfrak{F}_p$ is always contained in the linear fiber $\mathfrak{L}_p$.

For both $X = \mathbb{P}^1_k \times \mathbb{P}^1_k$ and $X = \mathbb{P}^2_k$, we give threshold degrees depending of the degree $(\boldsymbol{d}, e)$ of Ψ_i's. Beyond these threshold degrees, let's denote them as $(\boldsymbol{\mu}, \nu)$, Hilbert function of the linear fiber at p evaluated at $(\boldsymbol{\mu}, \nu)$, denoted by $HF_{\mathrm{Sym}(I)\otimes\kappa(p)}(\boldsymbol{\mu}, \nu)$ is equal to Hilbert polynomial of the linear fiber at p evaluated at $(\boldsymbol{\mu}, \nu)$, denoted by $HP_{\mathrm{Sym}(I)\otimes\kappa(p)}(\boldsymbol{\mu}, \nu)$. In the case where the fiber π_2^{-1} is finite, $HP_{\mathrm{Sym}(I)\otimes\kappa(p)}(\boldsymbol{\mu}, \nu)$ is nothing but the degree of the linear fiber at p, which implies it is the number of the orthogonal projections of p onto the given surface. For this reason, we study the vanishings of the local cohomology modules of the linear fiber over the irrelevant ideal $B = (\underline{x}) \cdot (t, \bar{t})$ of the ring R. Moreover, we fill a matrix with syzygies of I at degree beyond the threshold degree. We denote this matrix as $\mathbb{M}_{(\boldsymbol{\mu},\nu)}(\Psi)$. Then, for any point $p \in \mathbb{P}^3_k$ the corank of the matrix evaluated at p, denoted as $\mathbb{M}_{(\boldsymbol{\mu},\nu)}(p)$, is equal to the Hilbert function of the linear fiber at p in degree $(\boldsymbol{\mu}, \nu)$.

Similar to the work [24], the study of linear fiber of the rational map Ψ defined as before requires some assumptions on dimension one components of the base locus $\mathcal{B}$ of Ψ. For this purpose, we introduce the following definition.

Definition. A curve $\mathcal{C} \subset X \times \mathbb{P}^1_k$ is said to have *no section in degree* $< (\boldsymbol{a}, b)$ if $H^0(\mathcal{C}, \mathcal{O}_\mathcal{C}(\boldsymbol{\alpha}, \beta)) = 0$ for any degree $(\boldsymbol{\alpha}, \beta)$ such that $\boldsymbol{\alpha} < \boldsymbol{a}$ and $\beta < b$, i.e. if $\mathcal{C}$ has no global section in degree $< (\boldsymbol{a}, b)$.

Lastly before giving our main results, for simplicity we introduce a notation :

Notation. Let r be a positive integer. For any $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_r) \in (\mathbb{Z} \cup \{-\infty\})^r$ we set

$$\mathbb{E}(\boldsymbol{\alpha}) := \{\boldsymbol{\zeta} \in \mathbb{Z}^r \mid \zeta_i \geqslant \alpha_i \text{ for all } i = 1, \ldots, r\}.$$

It follows that for any $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ in $(\mathbb{Z} \cup \{-\infty\})^r$ we have that $\mathbb{E}(\boldsymbol{\alpha}) \cap \mathbb{E}(\boldsymbol{\beta}) = \mathbb{E}(\boldsymbol{\gamma})$ where $\gamma_i = \max\{\alpha_i, \beta_i\}$ for all $i = 1, \ldots, r$, i.e. $\boldsymbol{\gamma}$ is the maximum of $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ component-wisely.

Main result 3.(Theorem 3.2.1) Assume that we are in one of the two following cases:

(a) The base locus $\mathcal{B}$ is finite, possibly empty,

(b) $\dim(\mathcal{B}) = 1$, the top unmixed one-dimensional curve component $\mathcal{C}$ of $\mathcal{B}$ has no section in degree $< (\mathbf{0}, e)$ and $I^{\text{sat}} = I'^{\text{sat}}$ where I' is an ideal generated by three general linear combinations of the polynomials $\Psi_0, \ldots, \Psi_3$.

Let p be a point in $\mathbb{P}^3_k$ such that $\mathfrak{L}_p$ is finite, then

$$\operatorname{corank} \mathbb{M}_{(\boldsymbol{\mu},\nu)}(p) = \deg(\mathfrak{L}_p)$$

for any degree $(\boldsymbol{\mu}, \nu)$ such that

- if $X = \mathbb{P}^2_k$,
$$(\boldsymbol{\mu}, \nu) \in \mathbb{E}(3d - 2, e - 1) \cup \mathbb{E}(2d - 2, 3e - 1).$$
- if $X = \mathbb{P}^1_k \times \mathbb{P}^1_k$,
$$(\boldsymbol{\mu}, \nu) \in \mathbb{E}(3d_1 - 1, 2d_2 - 1, e - 1) \cup \mathbb{E}(2d_1 - 1, 3d_2 - 1, e - 1) \cup \mathbb{E}(2d_1 - 1, 2d_2 - 1, 3e - 1).$$

Our motivation to study the fibers of multi-graded rational map Ψ is to compute the orthogonal projections of a point in $\mathbb{P}^3_k$ onto a given surface. However, the hypothesis $I^{\text{sat}} = I'^{\text{sat}}$ where I' is an ideal generated by three general linear combinations of the polynomials $\Psi_0, \ldots, \Psi_3$ is rarely fulfilled, particularly if Ψ is a parameterization of the congruence of normal lines to a given surface. For that reason, we use explicitely the fact that the base locus $\mathcal{B}$ of Ψ has a known dimension one component in order to compute the degree of linear fiber. Let's denote the top unmixed one-dimensional curve component of $\mathcal{B}$ by $\mathcal{C}$.

Main result 4.(Theorem 3.2.2) Assume that $\dim(\mathcal{B}) = 1$ and that $\mathcal{C}$ has no section in degree $< (\mathbf{0}, e)$. Moreover, assume that there exists an homogeneous ideal $J \subset R$ generated by a regular sequence (g_1, g_2) such that $I \subset J$ and $(I : J)$ defines a finite subscheme in $X \times \mathbb{P}^1_k$. Denote by $(\boldsymbol{m}_1, n_1)$, resp. $(\boldsymbol{m}_2, n_2)$, the degree of g_1, resp. g_2. If $X = \mathbb{P}^2_k$ then $\boldsymbol{m_1}, \boldsymbol{m_2}$ are degrees, if $X = \mathbb{P}^1_k \times \mathbb{P}^1_k$ then $\boldsymbol{m_1}, \boldsymbol{m_2}$ are bidegrees such that $\boldsymbol{m_1} = (m_{1,1}, m_{1,2})$ and $\boldsymbol{m_2} = (m_{2,1}, m_{2,2})$. Set $\eta := \max(e - n_1 - n_2, 0)$ and let p be a point in $\mathbb{P}^3_k$ such that $\mathfrak{L}_p$ is finite. Then,

$$\operatorname{corank} \mathbb{M}_{(\boldsymbol{\mu},\nu)}(p) = \deg(\mathfrak{L}_p)$$

for any degree $(\boldsymbol{\mu}, \nu)$ such that

(a) if $X = \mathbb{P}^2_k$

$$(\mu, \nu) \in \mathbb{E}(3d - 2, e - 1 + \eta) \cup \mathbb{E}(3d - 2 - \min\{\boldsymbol{m_1}, \boldsymbol{m_2}\}, 3e - 1).$$

(b) if $X = \mathbb{P}^1_k \times \mathbb{P}^1_k$

$$(\boldsymbol{\mu}, \nu) \in \mathbb{E}(3d_1 - 1, 2d_2 - 1 + \tau_2, e - 1 + \eta) \cup \mathbb{E}(2d_1 - 1 + \tau_1, 3d_2 - 1, e - 1 + \eta) \cup \mathbb{E}(2d_1 - 1 + \tau_1, 2d_2 - 1 + \tau_2, 3e - 1),$$

where $\tau_i := d_i - \min\{2m_{1,i} + m_{2,i}, m_{i,1} + 2m_{2,i}, d_i\} \geqslant 0,\ i = 1, 2.$

In the same chapter, the computation of $\mathbb{M}_{(\boldsymbol{\mu},\nu)}(\Psi)$ is described as a null space of a linear system, and corresponding MACAULAY2 code is also given with. We emphasize that the matrix $\mathbb{M}_{(\boldsymbol{\mu},\nu)}(\Psi)$ does not depend on the chosen point p in $\mathbb{P}^3_k$. Namely, once we compute it, we store and use it for any p in $\mathbb{P}^3_k$. After computing the matrix $\mathbb{M}_{(\boldsymbol{\mu},\nu)}(\Psi)$, for any point p in $\mathbb{P}^3_k$ having finite fiber, we describe how to compute the coordinates of the orthogonal projections of p onto the given surface by using generalized eigenvalues and eigenvectors computations. Even if we introduce a new algebraic method, it allows the use of numerical approximations, i.e. floating-point data relying on numerical linear algebra. Lastly, we observe that the computations over the rational field takes much more time than the computations on floating points, since the coefficients get bigger along the calculations. For that reason, we give a bound for the height of the matrix $\mathbb{M}_{(\boldsymbol{\mu},\nu)}(\Psi)$, in terms of the height of Ψ with respect to p-adic and absolute valuation, degree of the polynomials which define the parameterization of the given surface and the degree $(\boldsymbol{\mu}, \nu)$.

Three-month industrial secondment at Missler Software

The appendix A consists of my technical report which explains two distance problems in space which I treated during my 3-month secondment in Missler Software in Toulouse in France based on some methods in symbolic computation. The aim of my stay was only to transfer some known algebraic approaches for solving the following problems. Problem 1 is the distance between a circle and a line in 3D and Problem 2 is the distance between an arc of a circle and a line segment in three dimensional space. These problems were chosen to improve some existing algorithms in terms of accuracy and the time computation. Since, after all experiments we have seen that the new algorithms are faster and they get more accurate solutions, I have integrated the algorithms into the interface of TopSolid. They are going to be used in the next version of TopSolid.

Firstly, two implemented algorithms in the CAD Software TopSolid (in programming language C#) to compute the distance between a circle and a line in space are described briefly. One of the algorithms depends on the parameter value of the circle and the other one depends on the parameter value of the line.

After that, my new algorithm for the distance between a line and a circle is explained (see Algorithm 3). Algorithm 3 handles the problem in three different cases : the line is perpendicular to the plane where the circle is located, the line is in the same plane as the circle, and the other situations. First two cases use the elementary Euclidean geometry, and the third case studies the resultant of two partial derivatives of the distance function between a circle and a line. This particular problem of distance yields a resultant which is a univariate polynomial of degree four (see §A.3.3). I had two main reasons to split the algorithm into several cases. First, the elementary geometry is enough for first two cases, and second the computation time for them using elementary geometry is faster. In section §A.3.4, the number of

the real solutions of such a resultant is studied by Theorem A.3.1 which is a root classification of a polynomial of degree four.

Then, my new algorithm for the distance between an arc of a circle and a line segment is described in Algorithm 4. This algorithm is based on each critical points of the distance between the circle containing the given arc and the line containing the given line segment, which are the extremities of the arc and the segment with the parameter values that are obtained by the resultant.

Lastly, the computational observations such as tolerance choice at several steps in the algorithms are explained. The comparisons between existing algorithms and the algorithms that I implemented are described with some examples (see §A.7).

CHAPTER 1

Preliminaries

In this chapter, we give some basic constructions with their known properties which are all necessary for the following chapters, such as closed image and fiber of a rational map, blow-up algebras. After that, in order to approximate blow-up algebras we describe approximation complexes, generalized Koszul complex, Čech complex and local cohomology, spectral sequences and their convergence. In addition, we give some necessary definitions for height computation in order to give some complexity for our computation over $\mathbb{Q}$.

1.1 Closed image and fibers of rational maps

Let $R := k[x_0, \ldots, x_n] = k[\underline{x}]$ and $R' = k[T_0, \cdots, T_m] = k[\underline{T}]$ be the standard graded polynomial rings over a field k. We are given a rational map

$$\begin{aligned} \Phi : \quad \mathbb{P}_k^n \quad &\dashrightarrow \mathbb{P}_k^m \\ (x_0 : \cdots : x_n) \quad &\mapsto (F_0(\underline{x}) : \cdots : F_m(\underline{x}))\,, \end{aligned} \tag{1.1}$$

where $F_0, \cdots, F_m$ are homogeneous polynomials in $x_0, \ldots, x_n$ of the same degree d greater or equal to 1. Let I be the ideal in R generated by $F_0, \cdots, F_m$, $\mathfrak{m} := (x_0, \ldots, x_n)$ be the irrelevant ideal of R. Let $S := R \otimes R' = k[\underline{x}, \underline{T}]$ be the bi-graded polynomial ring over the field k with canonical grading $\deg(x_i) = (1, 0)$ and $\deg(T_j) = (0, 1)$ for $i = 0, \cdots n$ and $j = 0, \ldots, m$.

The graph of the rational map Φ as in (1.1) is the closure of the set

$$\{(x_0 : \ldots : x_n) \times \Phi(x_0 : \cdots : x_n) : (x_0 : \ldots : x_n) \times \Phi(x_0 : \cdots : x_n) \in (\mathbb{P}_k^n \backslash V(F_0, \ldots, F_m)) \times \mathbb{P}_k^m\},$$

denoted by Γ_Φ, from which we have two canonical projections, first one is on the first component, i.e. $\pi_1 : \Gamma_\Phi \to \mathbb{P}_k^n$, the second one is on the last component, i.e. $\pi_2 : \Gamma_\Phi \to \mathbb{P}_k^m$.

$$\begin{array}{ccc} \Gamma_\Phi & \hookrightarrow & \mathbb{P}_k^n \times \mathbb{P}_k^m \\ {\scriptstyle \pi_1}\downarrow & \nearrow_{\pi_2} & \\ \mathbb{P}_k^n & \overset{\Phi}{\dashrightarrow} & \mathbb{P}_k^m \end{array} \tag{1.2}$$

We know that the closure of the image of the rational map Φ is the image of its graph Γ_ϕ via π_2 (see [46]). Also, by the above diagram, we define the *fiber of a point* p in

$\mathbb{P}^m_k$ as the pre-images along π_2 of p, i.e. $\pi_2(p)^{-1} \subset \mathbb{P}^m_k$. More precisely, the fiber at point $p \in \mathbb{P}^m$ is the subscheme

$$\mathfrak{F}_p := \pi_2(p)^{-1} = \mathrm{Proj}(\mathrm{Rees}(I) \otimes \kappa(p)) \subset \mathbb{P}^n_k \times \mathbb{P}^m_k,$$

where $\kappa(p)$ is the residue field of p and $\mathrm{Rees}(I)$ denotes the Rees algebra of I, as explained in §1.2.

With a geometric point of view, the surjective map $S \mapsto B = S/I$ induces the k-schemes inclusion

$$\mathrm{Proj}(B) \subset \mathbb{P}^n_k \times \mathbb{P}^m_k := \mathrm{Proj}(S).$$

Then, the definition ideal of the projection of $\mathrm{Proj}(B)$ in $\mathbb{P}^m_k$ via π_2 is

$$\begin{aligned}
\mathfrak{U} &= \ker\left(R' \to \textstyle\prod_{i=0}^3 B_{(T_i)}\right) \\
&= \{r \in R' : \exists n \in \mathbb{N} \quad r\mathfrak{m}^n =_B 0\} \\
&= (I :_S \mathfrak{m}^\infty) \cap R' \\
&= (I :_S \mathfrak{m}^\infty)_0 \text{ (with respect to the grading of } R = k[x]) \\
&= H^0_{\mathfrak{m}}(B)_0 \text{ (see §1.6.).}
\end{aligned}$$

1.2 Blow-up algebras

The defining equations of the graph Γ_Φ of Φ are known to be the equations of the multi-graded *Rees algebra of the ideal* I generated by the coordinates of Φ, i.e. $I := (F_0, \ldots, F_m)$, denoted by $\mathrm{Rees}(I)$. We recall that

$$\mathrm{Rees}(I) := \oplus_{i \geqslant 0} I^i t^i \subset R[t].$$

The Rees algebra $\mathrm{Rees}(I)$ inherits the multi-grading via the natural map

$$\begin{array}{rccc}
\alpha: & R[T_0, \ldots, T_m] & \to & \mathrm{Rees}(I) \subset R[t] \\
& T_i & \mapsto & F_i t.
\end{array}$$

We refer the reader to [48, 50, 80] for further details about Rees algebra.

Let $R' = k[T_0, \ldots, T_m]$, $S = R \otimes R'$ and $\ker(\alpha) = \mathfrak{p}$. The ideal $\mathfrak{p}$ is bigraded. We set $\mathfrak{p}_{(\mu,\nu)} \subset R_\mu \otimes_k R'_\nu$, namely μ is the degree with respect to R and ν is the degree with respect to R'. We have the S-ideal generated by the syzygies of the ideal $I := (F_0, \ldots, F_m)$,

$$(\mathfrak{p}_{(*,1)}) = (\{\sum_{i=0}^m g_i T_i : g_i \in R \text{ and } \sum_{i=0}^m g_i F_i = 0\}).$$

Moreover, we have the following surjective maps

$$S \to S/(\mathfrak{p}_{(*,1)}) \simeq \mathrm{Sym}(I) \text{ and } \mathrm{Sym}(I) \to \mathrm{Rees}(I) \simeq S/(\mathfrak{p}),$$

where $\mathrm{Sym}(I)$ is called the *symmetric algebra* of the ideal I.

1.3 Koszul complex

In what follows we give some basic constructions from homological algebra: Koszul complex and its generalizations, approximation complexes, Čech complex and local

cohomology modules. We refer the reader for instance to [42, Appendix §2F], [9, §1.6], [41, §17], [7, §9] for more details about Koszul complex.

Let R be a commutative ring, M be an R-module, and $\varphi : M \to R$ be an R-linear map.

Definition 1.3.1 ([9, §1.6]). *The complex*

$$\cdots \to \bigwedge^n M \xrightarrow{d_\varphi} \bigwedge^{n-1} \to \cdots \to \bigwedge^2 M \xrightarrow{d_\varphi} \bigwedge^1 M \xrightarrow{d_\varphi} R \to 0,$$

where the R-linear map $d_\varphi : \bigwedge^n M \to \bigwedge^{n-1} M$ is such that for all $x_1, \ldots, x_n$ in M,

$$d_\varphi(x_1 \wedge \cdots \wedge x_n) = \sum_{i=1}^{n} (-1)^{i+1} \varphi(x_i) x_1 \wedge \cdots \wedge \widehat{x_i} \wedge \cdots \wedge x_n$$

(where $\widehat{x_i}$ indicates that x_i is omitted from the exterior product), is called the Koszul complex of φ, denoted by $K_\bullet(\varphi)$. Thus, $K_i(\varphi) = \bigwedge^i M$.

One can easily show that d_φ is a differential i.e, $d_\varphi \circ d_\varphi = 0$. Also it is an antiderivation of degree -1, i.e. $d_\varphi(x \wedge y) = d_\varphi(x) \wedge y + (-1)^{\deg(x)} x \wedge d_\varphi(y)$ for all homogeneous $x, y \in M$. Moreover, if N is an R-module, then $K_\bullet(\varphi) \otimes_R N$ is the Koszul complex of φ with coefficients in N, denoted by $K_\bullet(\varphi, N)$. Thus, we have $K_0(\varphi, N) = R$, $K_1(\varphi) = N$.

Definition 1.3.2 ([9, §1.6]). *Let M be a finite free R-module with basis $e_1, \ldots, e_n$. Then, a linear map $\varphi : M \to R$ is uniquely determined by $x_i = \varphi(e_i)$ for all $i = 1, \ldots, n$. Conversely given a sequence $\boldsymbol{x} = x_1, \ldots, x_n$, there exists a linear form φ on M with $\varphi(e_i) = x_i$. Then, the Koszul complex of the sequence $\boldsymbol{x}$ is $K_\bullet(\boldsymbol{x}) := K_\bullet(\varphi)$. Moreover,*

$$K_\bullet(\boldsymbol{x}) \simeq K_\bullet(x_1, \ldots, x_{n-1}) \otimes K_\bullet(x_n) \simeq K_\bullet(x_1) \otimes \cdots \otimes K_\bullet(x_n).$$

We call $Z_\bullet(\varphi) = \ker(d_\varphi)$, $B_\bullet(\varphi) = \mathcal{I}m(d_\varphi)$, $H_\bullet(\varphi) = Z_\bullet(\varphi)/B_\bullet(\varphi)$ the cycle, boundary and the Koszul homology of φ, respectively. Similarly, for every R-module N, we call $Z_\bullet(\varphi, N) = Z_\bullet(\varphi) \otimes_R N$, $B_\bullet(\varphi, N) = B_\bullet(\varphi) \otimes_R N$ and $H_\bullet(\varphi, N) = Z_\bullet(\varphi, N)/B_\bullet(\varphi, N)$ the cycle, boundary and the Koszul homology of φ with coefficients in N, (in other words the i-th homology R-module of the Koszul complex $K_\bullet(\varphi, N)$). Thus, with the notation of Definition 1.3.2, $H_0(K_\bullet(\varphi)) = \operatorname{coker}(\varphi) = R/I$, where $I = (\boldsymbol{x})$ is the ideal of R.

Definition 1.3.3 ([9, p. 47]). *Let M be a finite free R-module with basis $e_1^*, \ldots, e_n^*$. The complex*

$$0 \xrightarrow{d_\varphi^*} (\bigwedge^0 M)^* \xrightarrow{d_\varphi^*} (\bigwedge^1 M)^* \xrightarrow{d_\varphi^*} \cdots \xrightarrow{d_\varphi^*} (\bigwedge^n M)^* \xrightarrow{d_\varphi^*} 0$$

together with the differential $d_\varphi^* : (\bigwedge^p M)^* \to (\bigwedge^{p+1} M)^*$ such that for all $i = 0, \ldots, n$

$$d_\varphi^*(e_{i_1}^* \wedge \cdots \wedge e_{i_p}^*) = \sum_{\forall j \in \{1,\ldots,n\} \setminus \{1,\ldots,i_p\}} (-1)^{j+1} x_j e_{i_1}^* \wedge \cdots \wedge e_{i_p}^* \wedge e_j^*$$

is a dual Koszul complex of φ, denoted by $K_\bullet(\boldsymbol{x}, M)^*$.

There exists a unique R-isomorphism $w_n : \bigwedge^n M \to R$, with $w_n(e_1 \wedge \cdots \wedge e_n) = 1$. $w_i : \bigwedge^i M \to (\bigwedge^{n-i} M)^*$ given by $(w_i(x))(y) = w_n(x \wedge y)$. In particular, it is the sign of the permutation of x, y for all $x \in \bigwedge^i M$, $y \in \bigwedge^{n-i} M$.

Proposition 1.3.1 ([42, Appendix §2F])**.** *Let $e_1, \ldots, e_n$ be a basis of M and $\{j_1, \ldots, j_{n-p}\}$ be the complement of $\{i_1, \ldots, i_p\} \in \{1, \ldots, n\}$. Then, $w_p := \bigwedge^p M \to (\bigwedge^{n-p} M)^*$*

$$w_p(e_{i_1} \wedge \ldots \wedge e_{i_p}) = \text{sign}(\sigma)(e^*_{j_1} \wedge \ldots \wedge e^*_{j_{n-p}})$$

where $\text{sign}(\sigma)$ is the sign of the permutation $\sigma = (i_1 \cdots i_p j_1 \cdots j_{n-p})$ defines an isomorphism.

Then, $e^*_{i+1}, \ldots, e^*_n$ is the dual basis of $e_1, \ldots e_i$ for $i = 1, \ldots n$ and we have the following commutative diagram.

$$\begin{array}{lccccccccc}
K_\bullet(\boldsymbol{x}): & 0 & \to & \bigwedge^n M & \xrightarrow{d_\varphi} & \bigwedge^{n-1} M & \cdots & \xrightarrow{d_\varphi} & \bigwedge^1 M & \xrightarrow{d_\varphi} & R \to 0 \\
 & & & \downarrow w_n & & \downarrow w_{n-1} & & & \downarrow w_1 & & \downarrow w_0 \\
K_\bullet(\boldsymbol{x})^*: & 0 & \to & (\bigwedge^0 M)^* & \xrightarrow{d^*_\varphi} & (\bigwedge^1 M)^* & \cdots & \xrightarrow{d^*_\varphi} & (\bigwedge^{n-1} M)^* & \xrightarrow{d^*_\varphi} & R \to 0
\end{array}$$

Example 1.3.1. *Let M be a finite free R-module with basis e_0, e_1, e_2, e_3. Then its Koszul complex is as follows*

$$0 \to \bigwedge^4 M \xrightarrow{\begin{bmatrix} -e_3 \\ e_2 \\ -e_1 \\ e_0 \end{bmatrix}} \bigwedge^3 M \xrightarrow{\begin{bmatrix} e_2 & e_3 & 0 & 0 \\ -e_1 & 0 & e_3 & 0 \\ 0 & -e_1 & -e_2 & e_3 \\ e_0 & 0 & 0 & -e_2 \\ 0 & 0 & e_0 & e_1 \end{bmatrix}} \bigwedge^2 M \tag{1.3}$$

$$\xrightarrow{\begin{bmatrix} -e_1 & -e_2 & -e_3 & 0 & 0 & 0 \\ e_0 & 0 & 0 & -e_2 & -e_3 & 0 \\ 0 & e_0 & 0 & e_1 & 0 & -e_3 \\ 0 & 0 & e_0 & 0 & e_1 & e_2 \end{bmatrix}} \bigwedge^1 M \quad (= M) \xrightarrow{\begin{bmatrix} e_0 & e_1 & e_2 & e_3 \end{bmatrix}} \bigwedge^0 M \quad (= R) \to 0.$$

Its dual Koszul complex is

$$0 \to (\bigwedge^0 M)^* \quad (= R) \xrightarrow{\begin{bmatrix} e_0 \\ e_1 \\ e_2 \\ e_3 \end{bmatrix}} (\bigwedge^1 M)^* \quad (= M^*) \xrightarrow{\begin{bmatrix} -e_1 & e_0 & 0 & 0 \\ -e_2 & 0 & e_0 & 0 \\ -e_3 & 0 & 0 & e_0 \\ 0 & -e_2 & e_1 & 0 \\ 0 & -e_3 & 0 & e_1 \\ 0 & 0 & -e_3 & e_2 \end{bmatrix}} (\bigwedge^2 M)^* \tag{1.4}$$

$$\xrightarrow{\begin{bmatrix} e_2 & -e_1 & 0 & e_0 & 0 \\ e_3 & 0 & -e_1 & 0 & 0 \\ 0 & e_3 & -e_2 & 0 & e_0 \\ 0 & 0 & e_3 & -e_2 & e_1 \end{bmatrix}} (\bigwedge^3 M)^* \xrightarrow{\begin{bmatrix} -e_3 & e_2 & -e_1 & e_0 \end{bmatrix}} (\bigwedge^4 M)^* \to 0.$$

Proposition 1.3.2 ([9, Proposition 1.6.10]). *With the previous notation,*

1. $K_\bullet(\boldsymbol{x})$ *and* $(K_\bullet(\boldsymbol{x}))^* = K^\bullet$ *are isomorphic; the Koszul complex is said to be self-dual.*
2. *For every R-module N, the complexes $K_\bullet(\boldsymbol{x}, N)$ and $K^\bullet(\boldsymbol{x}, N)$ are isomorphic.*
3. $H_i(\boldsymbol{x}, N) \simeq H^{n-i}(\boldsymbol{x}, N)$, *for all* $i = 0, \ldots, n$.

Proposition 1.3.3 ([9, Proposition 1.6.5.(b)]). *Let I be $\mathcal{I}m(\varphi)$, then I annihilates $K_\bullet(\varphi)$, $K_\bullet(\varphi, N)$, $K^\bullet(\varphi)$, $K^\bullet(\varphi, N)$. Furthermore, the annihilator of N annihilates $K_\bullet(\varphi, N)$, $K^\bullet(\varphi, N)$.*

Definition 1.3.4 ([9, Definition 1.1.1]). *A sequence $\boldsymbol{x} = x_1, \ldots, x_n$ of elements in R is called a weak M-sequence if x_i is not a zero divisor on $M/(x_1, \ldots, x_{n-1})M$ for $i = 1, \ldots n$. Moreover, $\boldsymbol{x}$ is called a M-regular sequence if it is a weak M-sequence and $M/\boldsymbol{x}M \neq 0$.*

Proposition 1.3.4 ([41, §17.2]). *If $\boldsymbol{x}$ is a M-regular sequence, then $K_\bullet(\boldsymbol{x}, M)$ is acyclic*

$$H_i(\boldsymbol{x}, M) = 0 \text{ for all } i \geqslant 1.$$

We refer the reader to [41, §17.2] for details about M-regular sequences and Koszul homology, to [41, §2.2] for details about Hom functor, and to [41, §A3.11] or [60, §IV.1] for Ext functor.

Theorem 1.3.1 ([9, Theorem 1.6.16]). *With the previous notation, if $I = (\boldsymbol{x})$ contains a weak M-sequence $\boldsymbol{y} = y_1, \ldots, y_m$, then*

$$H_{n+1-m}(\boldsymbol{x}, M) = 0 \text{ for } i = 1, \ldots, m \text{ and}$$

$$H_{n-m}(\boldsymbol{x}, M) \simeq \mathrm{Hom}_R(R/I, M/\boldsymbol{y}M) \simeq \mathrm{Ext}^m_R(R/I, M).$$

Corollary 1.3.1 ([9, Corollary 1.6.13]). *Using the previous notation,*

1. *Set $\boldsymbol{x} = x_1, \ldots, x_{n-1}$. Then, we have an exact sequence*

$$\cdots \xrightarrow{\pm x_n} H_i(\boldsymbol{x}', M) \to H_i(\boldsymbol{x}, M) \to H_{i-1}(\boldsymbol{x}', M) \xrightarrow{\pm x_n} H_{i-1}(\boldsymbol{x}', M) \to \cdots$$

2. *Let $p \leqslant n$, $\boldsymbol{x}' = x_1, \ldots, x_p$ and $\boldsymbol{x}'' = x_{p+1}, \ldots, x_n$. If $\boldsymbol{x}'$ is weakly M-regular, then one has an isomorphism*

$$H_\bullet(\boldsymbol{x}, M) \simeq H_\bullet(\boldsymbol{x}'', M/\boldsymbol{x}'M).$$

1.4 Approximation complexes

In this section we introduce approximation complexes with some basic properties such as their acyclicity. They have been firstly introduced in [49]. We refer the reader to [80, 48, 50] for further details.

Let k be a field, $k[x_0,\dots,x_n] = k[\boldsymbol{x}]$ be the coordinate ring of $\mathbb{P}^n_k$ and R be the ring $k[T_0,\dots,T_m] = k[\boldsymbol{T}]$. Consider two Koszul complexes over the ring $S = k[x_0,\dots,x_n] \otimes k[T_0,\dots,T_m] = k[\boldsymbol{x},\boldsymbol{T}]$ associated to the sequences of homogeneous polynomials $\boldsymbol{F} := (F_0,\dots,F_m)$, where F_i's are in $k[\boldsymbol{x}]$ for all $i = 0,\dots,m$ and also to $T_0,\dots,T_m$. We denote these Koszul complexes by $K_\bullet(\boldsymbol{F},S)$ and $K_\bullet(\boldsymbol{T},S)$ with the corresponding differentials $d^{\boldsymbol{F}}$ and respectively $d^{\boldsymbol{T}}$. The last differentials of these two Koszul complexes are as follows

$$\begin{array}{rccc} d_1^{\boldsymbol{F}}: & S^m & \xrightarrow{(F_0,\dots,F_m)} & S \\ & (g_0,\dots,g_m) & \mapsto & \sum_{i=0}^m g_iF_i, \\ d_1^{\boldsymbol{T}}: & S^m & \xrightarrow{(T_0,\dots,T_m)} & S \\ & (g_0,\dots,g_m) & \mapsto & \sum_{i=0}^m g_iT_i, \end{array}$$

One can easily check that $d^{\boldsymbol{F}}$ and $d^{\boldsymbol{T}}$ verifies $d^{\boldsymbol{F}} \circ d^{\boldsymbol{T}} + d^{\boldsymbol{T}} \circ d^{\boldsymbol{F}}$ which gives rise to a double complex $K_\bullet(\boldsymbol{x},\boldsymbol{T};S)$. We set Z_i, B_i and H_i for the cycles, boundaries and the homology modules of $K_\bullet(\boldsymbol{F},S)$ respectively. From them, $d^{\boldsymbol{T}}$ induces $\mathcal{Z}_\bullet = (\ker(d^{\boldsymbol{F}}), d^{\boldsymbol{T}})$, $\mathcal{B}_\bullet = (\mathcal{I}m(d^{\boldsymbol{F}}), d^{\boldsymbol{T}})$ and lastly $\mathcal{M}_\bullet = (H_\bullet(K_\bullet(\boldsymbol{F},S)), d^{\boldsymbol{T}})$ the cycles, boundaries and the homology modules of approximation complexes respectively.

Consider the end of $\mathcal{Z}_\bullet$, i.e.

$$\ker(d_1^{\boldsymbol{F}}) \xrightarrow{d_1^{\boldsymbol{T}}} S \to 0.$$

By definition, we have

$$d_1^{\boldsymbol{T}}(\ker(d_1^{\boldsymbol{F}})) = \{\sum_{i=0}^m g_iT_i : \sum_{i=0}^m g_iF_i = 0\},$$

which implies that

$$H_0(\mathcal{Z}_\bullet) = \frac{S}{d_1^{\boldsymbol{T}}(\ker(d_1^{\boldsymbol{F}}))} \simeq \mathrm{Sym}(I), \text{ (see §1.2 for Sym}(I)\text{)}$$

where I is the ideal generated by $F_0,\dots,F_m$. More precisely, the $\mathcal{Z}_\bullet$ gives an approximation for symmetric algebra of I with respect to the ring S.

Proposition 1.4.1. *With previous notation, the modules $\mathcal{Z}_i$, $\mathcal{B}_i$ and $\mathcal{M}_i$ for all i do not depend on the chosen generating set of the ideal I of R.*

Proof. See Proposition 3.2.6 and Corollary 3.2.7 in [80] or [49, §3]. □

Proposition 1.4.2. *Assume S is a noetherian ring and $i \geqslant 1$. If $H_i(\mathcal{M}) = 0$ then $H_i(\mathcal{Z}) = 0$. In particular, if $\mathcal{M}$ is acyclic then $\mathcal{Z}$ is also acyclic.*

Proof. See [14, Proposition 4.3]. □

Proposition 1.4.3. *If $H_1(\mathcal{M}) = 0$, then $\mathrm{Sym}(I) \simeq \mathrm{Rees}(I)$.*

Proof. See [14, Proposition 4.5] or [80]. □

1.5 Generalized Koszul complex

Before presenting the generalized Koszul complex, we need to introduce determinantal ideals (see [41, 69]). Let M and N be R-modules. Let the notation $(-)^*$ stands for the dual, i.e. $N^* = \mathrm{Hom}_R(N, R)$. For further details about generalized Koszul complex, we refer the reader to for instance [42, Appendix §2H], [41, Appendix §2.6] or [10, 40].

Definition 1.5.1 ([41, §20.2]). *If $\varphi : M \to N$ is a map of free modules, then $I_j(\varphi)$ is the image of the map*

$$\wedge^j M \otimes \wedge^j N^* \to R$$

induced by $\wedge^j \varphi : \wedge^j M \to \wedge^j N$. If we choose bases for M and N, then φ might be represented by a matrix and $I_j(\varphi)$ is generated by the $j \times j$-minors of this matrix. By convention, determinant of 0×0-matrix is 1, also $I_j(\varphi) = R$ for $I_j \leqslant 0$.

These ideals are invariants:

Corollary 1.5.1 ([41, Corollary-Definition 20.4]). *Let M be a finitely generated R-module, and let $\varphi : F \to G \to M \to 0$ and $\varphi' : F' \to G' \to M \to 0$ be any two presentations with G and G' finitely generated free modules of rank r and r', respectively. For each non-negative integer i, we have*

$$I_{r-i}(\varphi) = I_{r'-i}(\varphi').$$

Definition 1.5.2. *With previous notation, we define i-th Fitting invariant of M to be the ideal*

$$I_{r-i}(\varphi) \subset R.$$

We have seen that Koszul complex corresponds to a map from finitely generated free module over a given ring R to R, i.e. to $\varphi : M \to R$, where M is a finitely generated R-module. In this section, we generalize Koszul complex to the complexes associated to a map of finitely generated free modules over R, i.e. to $\varphi : M \to N$, where M and N are finitely generated R-modules. Let M and N be of rank m and n, respectively. Assume that $m \geqslant n$. Then, these new complexes are in strong relation with the determinantal ideal $I_n(\varphi)$ of maximal minors of φ. Let $\mathcal{S}_i(N)$ denotes the i-th symmetric power of N (see [41, Appendix §2.3]).

Definition 1.5.3 ([42, Appendix §2H]). *We define the complex*

$$0 \to (\mathcal{S}_{m-n}(N))^* \otimes \wedge^m M \xrightarrow{\delta_{m-n+1}} (\mathcal{S}_{m-n-1}(N))^* \otimes \wedge^{m-1} \xrightarrow{\delta m-n}$$

$$\cdots \xrightarrow{\delta_2} N^* \otimes \wedge^{n+1} M \xrightarrow{\delta_1} \wedge^n M \xrightarrow{\epsilon} R,$$

where

(a) the map ϵ is identified with the map $\wedge^n M \xrightarrow{\wedge^n \varphi} \wedge^n N \simeq R$, whose image is the ideal generated by $n \times n$-minors of φ,

(b) the map δ is defined as follows. Firstly, we define

$$\Delta : (\mathcal{S}_k(N))^* \to N^* \otimes (\mathcal{S}_{k-1}(N))^*$$

as the dual of the multiplication map $N \otimes \mathcal{S}_{k-1}(N) \to \mathcal{S}_k(N)$ *in symmetric algebra of* N*. Analogously we define the map*

$$\Delta : \wedge^k M \to M \otimes \wedge^{k-1} M$$

as the dual of the multiplication in the exterior algebra of M^**. For* $u \in (\mathcal{S}_{j-1}(N))^*$ *we write* $\Delta(u) = \sum_i u'_i \otimes u''_i \in N^* \otimes (\mathcal{S}_{j-2}(N))^*$ *and similarly for* $v \in \wedge^{n+j-1} M$ *we write* $\Delta(v) = \sum_t v'_t \otimes v''_t \in M \otimes \wedge^{n+j-2} M$*. Let's note that* $\alpha^*(u'_s) \in M^*$*, so* $[\alpha^*(u'_i)](v'_t) \in R$*. Then, we set*

$$\begin{array}{rccl} \delta_j : & (\mathcal{S}_{j-1}(N))^* \otimes \wedge^{n+j-1} M & \to & (\mathcal{S}_{j-2}(N))^* \otimes \wedge^{n+j-2} M \\ & u \otimes v & \mapsto & \sum\limits_{s,t} [\alpha^*(u'_s)](v'_s) \dot{u}''_s \otimes v''_t. \end{array} \tag{1.5}$$

This complex is called the Eagon-Northcott complex of φ*, denoted by* $\boldsymbol{EN}(\varphi)$*.*

Now, we will define a complex which can be thought as an approximation of a resolution of the cokernel of the map of finitely generated R-modules, $\varphi : M \to N$.

Definition 1.5.4 ([41, Appendix §2.6.1])**.** *We define the complex*

$$0 \to (\mathcal{S}_{m-n-1}(N))^* \otimes \wedge^m M \xrightarrow{\delta_{m-n}} (\mathcal{S}_{m-n-2}(N))^* \otimes \wedge^{m-2} M \xrightarrow{\delta_{m-n-1}}$$

$$\cdots \xrightarrow{\delta_1} \wedge^{n+1} M \xrightarrow{\epsilon} M \xrightarrow{\varphi} N.$$

where

(a) the map δ *is similar to the map* δ *as in Definition 1.5.3, (It may be described by the multiplication* $a \in N \otimes N^* \subset \mathcal{S}(N) \otimes \wedge N^*$*.)*

(b) the map ϵ *is the action of* $\wedge^n \varphi^* \gamma$ *on* M*, where* $\gamma \in \wedge^n N^* \simeq R$*. (Such a map* γ *might be chosen because we have assumed that* N *is a free module.)*

This complex is called the Buchsbaum-Rim complex of φ*, denoted by* $\boldsymbol{BR}(\varphi)$*.*

Theorem 1.5.1 ([41, Theorem A2.10])**.** *The Eagon-Northcott complex and the Buchsbaum-Rim complex of* φ*, as defined above, are exact and provide free resolutions of* $R/I_m(\varphi)$ *if and only if* $I_m(\varphi)$ *contains a regular sequence of length* $m - n + 1$*.*

Example 1.5.1 ([42, Appendix §2.65])**.** *With the previous notation, let* $\operatorname{rank}(N) = n = 1$*. Then, we can identify* N*, its symmetric powers* $\mathcal{S}_k(N)$ *and their duals* $(\mathcal{S}_k(N))^*$ *with* R*. Thus, the Eagon-Northcott complex in this case is nothing but the Koszul complex of* $\varphi : M \to R \quad (\simeq \wedge^1 N)$*.*

1.6 Čech Complex and local cohomology

Let R be a ring, $\boldsymbol{x} = x_1, \ldots, x_n$ be a sequence in R and M be a R-module.

Definition 1.6.1 ([8, Proposition and Definition 5.1.5])**.** *We define a complex* $\check{\mathscr{C}}^\bullet(\boldsymbol{x}, M)$*, or simply* $\check{\mathscr{C}}^\bullet(M)$*, of* R*-modules and* R*-homomorphisms as follows*

$$0 \to \check{\mathscr{C}}^0(M) \xrightarrow{d_0} \check{\mathscr{C}}^1(M) \to \cdots \to \check{\mathscr{C}}^{n-1} \xrightarrow{d^{n-1}} \check{\mathscr{C}}^n(M) \to 0,$$

with

(a) $\check{\mathscr{C}}^0(M) := M$,

(b) $\check{\mathscr{C}}^k(M) := \bigoplus_{1\leqslant i_1<\cdots<i_k\leqslant n} M_{x_{i_1}x_{i_2}\cdots x_{i_k}}$, *for all* $k = 1, \ldots, n$,

(c) $d^0 : \check{\mathscr{C}}^0(M) \to \check{\mathscr{C}}^1(M)$ *is such that for each* $h = 1, \ldots, n$ *the composition of* d^0 *followed by the canonical projection from* $\check{\mathscr{C}}^1(M)$ *to* M_{x_h} *is natural map from* M *to* M_{x_h} *(i.e. localization and* $d^0(m) = \sum_{i=1}^{n} \frac{m}{1}$ *for* $m \in M$*); and*

(d) $d^h(m_{i_1\cdots i_h}) = \sum_{k\notin i_1,\ldots,i_h} (-1)^{s(k)}\phi_k(m_{i_1\cdots i_h})$, *where* $i_{s(k)} < k < i_{s(k)+1}$ *and* $\phi_k(m_{i_1\cdots i_h}) \in M_{x_{i_1}\cdots x_{i_h}\cdots x_{i_h}}$.

Then, the complex $\check{\mathscr{C}}^\bullet(M)$ *is called the Čech complex of* M *with respect to* $x_1, \ldots, x_n$.

Example 1.6.1 ([8, Example 5.1.6])**.** *Let us write the differentials of Čech complex* $\check{\mathscr{C}}^\bullet = \check{\mathscr{C}}^\bullet(R)$ *with respect to* x_1, x_2, x_3. *Then, the Čech complex is*

$$0 \to R \xrightarrow{d^0} R_{x_1} \oplus R_{x_2} \oplus R_{x_3} \xrightarrow{d^1} R_{x_2x_3} \oplus R_{x_1x_3} \oplus R_{x_1x_2} \xrightarrow{d^2} R_{x_1x_2x_3} \to 0,$$

where the differentials d^0, d^1, d^2 *are described as follows for* $r, r_1, r_2, r_3 \in R$ *and* $n_1, n_2, n_3 \in \mathbb{N}_*$.

$$d^0(r) = \left(\frac{r}{1}, \frac{r}{1}, \frac{r}{1}\right),$$

$$d^1\left(\frac{r_1}{a_1^{n_1}}, \frac{r_2}{a_2^{n_2}}, \frac{r_3}{a_3^{n_3}}\right) = \left(\frac{a_2^{n_3}r_3}{(a_2a_3)^{n_3}} - \frac{a_3^{n_2}r_2}{(a_2a_3)^{n_2}}, \frac{a_1^{n_3}r_3}{(a_1a_3)^{n_3}} - \frac{a_3^{n_1}r_1}{(a_1a_3)^{n_1}}, \frac{a_1^{n_2}r_2}{(a_1a_2)^{n_2}} - \frac{a_2^{n_1}r_1}{(a_1a_2)^{n_1}}\right),$$

and lastly

$$d^2\left(\frac{r_1}{(a_2a_3)^{n_1}}, \frac{r_2}{(a_1a_3)^{n_2}}, \frac{r_3}{(a_1a_2)^{n_3}}\right) = \left(\frac{a_1^{n_1}r_1}{(a_1a_2a_3)^{n_1}} - \frac{a_2^{n_2}r_2}{(a_1a_2a_3)^{n_2}} + \frac{a_3^{n_3}r_3}{(a_1a_2a_3)^{n_3}}.\right)$$

Definition 1.6.2. *We define* the local cohomology modules of R-module M over $\boldsymbol{x}$ *as* $H^i_{\boldsymbol{x}}(M) = \ker(d^i)/\mathcal{I}m(d^{i-1})$ *where* d^i*'s are the differentials of Čech complex of* M *for all* $i = 0, \ldots, n$.

Let R be a standard graded polynomial ring over field k, M be a finitely generated graded R-module, $\mathfrak{m}$ be the irrelevant ideal of R. Then, we have the invariant

$$a_i(M) := \inf\{\mu : H^i_{\mathfrak{m}}(M)_\mu = 0\}.$$

Definition 1.6.3. *With the same notation, Castenuovo-Mumford regularity of* M *over* R *is defined by*

$$\operatorname{reg}(M) := \max_i\{a_i(M) + i\}.$$

Theorem 1.6.1 ([9, Theorem 3.5.8])**.** *Let* $(R, \mathfrak{m}, k)$ *be a Noetherian local ring and* M *be a finite* R*-module of depth* t *and dimension* d. *Then,*

(a) $H^i_{\mathfrak{m}}(M) = 0$ *for* $i < t$ *and* $i > d$,

(b) $H^t_{\mathfrak{m}}(M) \neq 0$ *and* $H^d_{\mathfrak{m}}(M) \neq 0$.

1.7 Spectral sequences and double complexes

In this section we recall spectral sequences with some properties such as vertical and horizontal filtrations of a double complex, convergence and comparison theorems. For further details, we refer the reader to [83, 41].

Definition 1.7.1 ([83, Example 1.2.4]). *A double complex in an abelian category $\mathcal{A}$ is a family $\{C_{p,q}\}$ of objects of $\mathcal{A}$, together with maps*

$$d^h : C_{pq} \to C_{p-1,q} \text{ and } d^v : C_{p,q} \to C_{p,q-1},$$

verifying $d^h \circ d^h = d^v \circ d^v = d^h \circ d^v + d^v \circ d^h = 0$.

Definition 1.7.2 ([41, Appendix §3.12]). *We define the total complex of C, denoted by $\mathrm{Tot}(C)$, with differential $d = d^h + d^v$ (as in Definition 1.7.1) is a complex whose k-th term is*

$$\oplus_{p+q=k} C_{pq}.$$

Definition 1.7.3 ([83, Definition 5.2.1]). *A homology spectral sequence (starting with E^a) in an abelian category $\mathcal{A}$ consists of the following data:*

1. *A family $\{E^r_{pq}\}$ of objects of $\mathcal{A}$ defined for all integers p, q, and $r \geqslant a$,*
2. *Maps $d^r_{pq} : E^r_{pq} \to E^r_{p-r,q+r-1}$ that are differentials in the sens that $d^r \circ d^r = 0$,*
3. *Isomorphisms between E^{r+1}_{pq} and the homology of E^r_{**} at the spot E^r_{pq}:*

$$E^{r+1}_{pq} \simeq \frac{\ker(d^r_{pq})}{\mathcal{I}m(d^r_{p+r,q-r+1})}.$$

The total degree of the term E^r_{pq} is $n = p + q$; the terms of total degree n line of slope -1, and each differential d^r_{pq} decreases the total degree by one.

Note that d^{i+1}_{pq} is defined on the kernel of d^i_{pq} with $i \leqslant 1$ and E^{r+1}_{pq} is a subquotient of E^r_{pq}. Let B^i_{pq} denotes $\mathcal{I}m(d^r_{pq})$ and Z^i_{pq} denotes $\ker(d^r_{pq})$. Then, we have the nested submodules

$$0 = B^1_{pq} \subset B^2_{pq} \subset \cdots \subset B^r_{pq} \subset \cdots \subset Z^r_{pq} \subset \cdots \subset Z^2_{pq} \subset Z^1_{pq} = E^1_{pq}$$

such that $E^i_{pq} = Z^i_{pq}/B^i_{pq}$ for each i.

E^n_{pq} can be seen as n-th order approximation of the homology of the total complex $Tot(E_{**})$. We will call E^r_{**} as r-th sheet of spectral sequences. Similarly, there exists a dual definition to Definition 1.7.3 for *cohomology spectral sequences*, for instance see [83, Definition 5.2.3].

Definition 1.7.4 ([83, §5.3]). *A homology spectral sequence is said to be bounded if for each n there are only finitely many nonzero terms of total degree n in E^a_{**}. If it is the case then for each p and q there is a r_0 such that $E^r_{pq} = E^{r+1}_{pq}$ for all $r \geqslant r_0$. We denote this limit term as E^∞_{pq}.*

We call a *filtration* F on a chain complex C, an ordered family of chain subcomplexes

$$\cdots \subset F_{p-1}C \subset F_pC \subset \cdots$$

of C (see [83, §5],[41, Appendix §3.13]).

Definition 1.7.5 ([83, Bounded Convergence 5.2.5]). *We say that a bounded spectral sequence converges to H_* if we are given a family of objects H_n in abelian category $\mathcal{A}$, each having a finite filtration (i.e. the filtration stabilizes.)*

$$0 = F_sH_n \subset \cdots \subset F_{p-1}H_n \subset F_pH_n \subset F_{p+1}H_n \subset \cdots \subset F_tH_n = H_n,$$

then we have

$$E^\infty_{pq} = F_pH_{p+q}/F_{p-1}H_{p+q}.$$

Set

$$B^\infty_{pq} = \cap^\infty_{r=0}B^r_{pq} \text{ and } Z^\infty_{pq} = \cup^\infty_{r=0}Z^r_{pq}$$

and then we have,

$$E^\infty_{pq} = Z^\infty_{pq}/B^\infty_{pq}.$$

Definition 1.7.6 ([83, Definition 5.4.2]). *A filtration on a chain complex C is called bounded if for each n there are integers $s < t$ such that $F_sC_n = 0$ and $F_tC_n = C_n$. In this case, there are only finitely many nonzero terms of total degree n in E^0_{**}, then the spectral sequence is also bounded.*

Let G be the total complex of double complex C, i.e. $G = \mathrm{Tot}(C)$. Then, there exist two filtrations on G, namely vertical and horizontal filtrations.

Definition 1.7.7 ([83, Definition 5.6.1]). *The vertical filtration of total complex G is defined by the subcomplexes denoted by ${}_{ver}G_p$, where ${}_{ver}G_p$ come from the columns of $C_{p,*}$. It gives rise to a spectral sequence ${}_{ver}G_p$, starting with C_{pq}.*

Definition 1.7.8 ([83, Definition 5.6.2]). *The horizontal filtration of total complex G is defined by the subcomplexes denoted by ${}_{hor}G_q$, where ${}_{hor}G_q$ come from the rows of $C_{*,q}$. It gives rise to a spectral sequence ${}_{hor}G_q$, starting with C_{qp} (it interchanges indices p and q).*

In what follows, we will call the row filtered or column filtered double complex as horizontal and vertical filtrations respectively (see [41, Appendix §3.13]).

In addition, we will mainly use the following theorem to compare row and column filtered spectral sequences of a given double complex:

Theorem 1.7.1 ([41, Theorem A3.24]). *Let $C = C_{pq}$ be a double complex, ${}_{hor}E^r$ and ${}_{ver}E^r$ be the horizontal and the vertical filtrations of the total complex $\mathrm{Tot}(C)$, respectively. The E^1 terms are bigraded with the components given by*

$${}_{hor}E^1_{pq} = H^q(C_{*,p}) \text{ and } {}_{ver}E^1_{pq} = H^q(C_{p,*}).$$

If $C_{i,j} = 0$ for all $i < 0$ or for all $j > 0$, then the horizontal spectral sequences ${}_{hor}E^r$ converges to $H^{p+q}(\mathrm{Tot}(C))$ and by symmetry, if $C_{i,j} = 0$ for all $i > 0$ or for all $j < 0$, then the vertical spectral sequences ${}_{ver}E^r$ converges to $H^{p+q}(\mathrm{Tot}(C))$.

1.8 Height computation

In what follows, we give some basic definitions of standard and p-adic valuations and absolute values, height of a finite set and a polynomial with respect to these valuations. In §2.5 and §3.5.1, we compute upper bounds for the height of some special matrices that we introduce in §2.2 and §3.2.2 respectively in order to give some complexity upper bounds.

Definition 1.8.1 ([27, Chapter 4]). *Let k be a field. An absolute value (standard absolute value) is a map*

$$\begin{array}{rccc} |.|: & k & \to & \mathbb{R}_{\geqslant 0} \\ & x & \mapsto & |x| \end{array}$$

satisfying for all $x, y \in k$

1. *$|x| = 0$ if and only if $x = 0$,*
2. *$|x \cdot y| = |x| \cdot |y|$,*
3. *$|x + y| \leqslant |x| + |y|$.*

The notation $|.|_\infty$ is also used for standard absolute value.

Definition 1.8.2 ([27, Chapter 4]). *Let p a prime number. The p-adic valuation is a map*

$$\begin{array}{rccc} v_p: & \mathbb{Q} & \to & \mathbb{Z} \cup \{\infty\} \\ & x & \mapsto & m, \end{array}$$

with $x = \frac{ap^m}{b}$ where a, b are integers such that $p \nmid a$, $p \nmid b$ satisfying for all $x, y \in \mathbb{Q}$

1. *$v_p(x) = \infty$ if and only if $x = 0$,*
2. *$v_p(x \cdot y) = v_p(x) + v_p(y)$,*
3. *$v_p(x + y) \geqslant \min\{v_p(x), v_p(y)\}$.*

Definition 1.8.3 ([27, Chapter 4]). *Let p be a prime number. The p-adic absolute value is defined as*

$$\begin{array}{rccc} |.|_p: & \mathbb{Q} & \to & \mathbb{Q}_{\geqslant 0} \\ & x & \mapsto & p^{-v_p(x)}, \end{array}$$

satisfying the three properties of an absolute value (given in the Definition 1.8.1).

Following the same notation of [57, §1.1.], there are p-adic absolute value, denoted by $|.|_p$, and the standard absolute value, denoted by $|.|_\infty$, over $\mathbb{Q}$. Let v be either ∞ or a prime number p. $\mathbb{Q}_v$ is defined to be the completion of $\mathbb{Q}$ with respect to the absolute value v. Also, $\mathbb{C}_v$ is defined to be the completion of the algebraic closure of $\mathbb{Q}_v$ with respect to the absolute value v (see [45, 21]).

Definition 1.8.4 ([57, §1.1.]). *Let S be a finite subset of $\mathbb{C}_v$, its absolute value is*

$$|S|_v := \max\{|s|_v : s \in S\},$$

and its height is

$$h_v(S) := \max\{0, \log|S|_v\}.$$

Proposition 1.8.1. *Let $S = \{s_1, \ldots, s_n\}$ be a finite set of $\mathbb{C}_v$, v stands for either ∞ or a prime number p, then we have*

1. $h_v(\sum_{i=1}^{n} s_i) = \max\{0, \log(|\sum_{i=1}^{n} s_i|_v)\} \leqslant \max\{0, \log(\sum_{i=1}^{n} |s_i|_v)\}$,
2. $h_v(\prod_{i=1}^{n} s_i) = \max\{0, \log(\prod_{i=1}^{n} |s_i|_v)\} = \max\{0, \sum_{i=1}^{n} \log|s_i|_v\}$.

Consider the polynomial

$$f = \sum_{\substack{0\leqslant\alpha_1,\cdots,\alpha_n\leqslant d \\ \alpha_1+\cdots+\alpha_n\leqslant d}} a_{\alpha_1\cdots\alpha_n} x_1^{\alpha_1}\cdots x_n^{\alpha_n} = \sum_{\alpha} \boldsymbol{a}_\alpha \boldsymbol{x}^\alpha$$

in $\mathbb{C}_v[x_1, \cdots, x_n]$ of total degree d.

Definition 1.8.5 ([57, §1.1.])**.** *The absolute value of the polynomial f, denoted by $|f|_v$, is defined to be the maximum absolute value of its set of coefficients, i.e.*

$$|f|_v := \max_{\alpha}\{|\boldsymbol{a}_\alpha|_v\}.$$

Definition 1.8.6 ([57, §1.1.])**.** *The height of the polynomial f, denoted by $h_v(f)$, is defined to be*

$$h_v(f) := \max\{0, \log(|f|_v)\}.$$

We notice that the height of a polynomial in $\mathbb{C}_v[x_1, \cdots, x_n]$ is always non-negative.

Notation 1.8.1. *Let F be the homogenization of f in $\mathbb{P}^n_{\mathbb{C}_\nu}$. Since the definition of height only considers the coefficients of f, we set*

$$h_v(F) = h_v(f).$$

CHAPTER 2

Curve implicitization

The main contribution of this chapter is a generalization of the method of moving conics [74] to the case of space curves, that we call the method of moving quadrics. In other words, we introduce a generalization to parameterized space curves of the hybrid Bézout matrix of a μ-basis. As in the case of plane curves, we will show that the gain in the size of the matrix is similar: for a general parameterized space curve, the size of the matrix of moving quadrics is about half of the size of the matrix of moving hyperplanes.

The chapter is organized as follows. In §2.1.1, we first revisit the method of moving conics [74] with a particular focus on Sylvester forms, a central construction of this chapter. In §2.1.2 we fix some notations and introduce the notion of moving hyperplanes and μ-basis for space curves. Then, in §2.2 we deal with the general case of parameterized curves in arbitrary dimension and state our main results. Their proofs have been concentrated in §2.3. After that, in §2.5, we give a upper height bound for the Hybrid Bézout matrix in any dimension in terms of the height of the parameterization of the curve. Finally, in §2.4 the effective computation of our new matrices is discussed and illustrated with some experiments. In particular, we illustrate the gain we obtain for the inversion of a point on the curve. This work is published in the proceeding of Symposium on Solid and Physical Modeling 2019 (see [20]).

2.1 Previous works on curve implicitization

2.1.1 Maps from $\mathbb{P}^1$ to $\mathbb{P}^2$

The implicitization of rational plane curves, that is to say the finding of an implicit equation of a plane curve from a parameterization, has been extensively studied in the past. Besides the basic method based on a resultant computation directly from a parameterization, the method of moving lines introduced by Sederberg and Chen in [73], and developed further with the concept of μ-basis in [31], has been the more powerful and fruitful one in geometric modeling. In this section, we briefly review it with a particular emphasis on its generalization to moving conics [74] that allows to obtain more compact matrices.

In what follows, we suppose that an homogeneous parameterization of a rational plane curve $\mathcal{C}$ is given over a field k by

$$\begin{aligned} \Phi : \quad \mathbb{P}^1 &\to \mathbb{P}^2 \\ (s:t) &\mapsto (f_0(s,t) : f_1(s,t) : f_2(s,t)), \end{aligned} \tag{2.1}$$

where f_0, f_1 and f_2 are homogeneous polynomials in $k[s,t]$ of the same degree $d \geqslant 1$. For the sake of simplicity, we assume that these polynomials have no common factor, so that the map Φ is well defined everywhere on $\mathbb{P}^1$.

Moving lines

A μ-basis of a rational plane curve is composed of two polynomial equations that both define a line in the plane that moves when the parameter of the curve moves [52, 26, 31].

Definition 2.1.1. *A* moving line *of degree $\nu \in \mathbb{N}$ is a polynomial of the form*

$$L(s,t;x_0,x_1,x_2) = g_0(s,t)x_0 + g_1(s,t)x_1 + g_2(s,t)x_2$$

where g_0, g_1 and g_2 are homogeneous polynomials in $k[s,t]$ of degree ν. For any point $(s_0 : t_0) \in \mathbb{P}^1$, $L(s_0,t_0;x_0,x_1,x_2)$ is a linear form in the variables x_0,x_1,x_2 that can be interpreted as the defining equation of a line in $\mathbb{P}^2$. This line moves when the point $(s_0 : t_0)$ varies in $\mathbb{P}^1$, hence its name. In addition, the moving line L is said to follow the parameterization Φ if

$$L(s,t;f_0(s,t),f_1(s,t),f_2(s,t)) = g_0f_0 + g_1f_1 + g_2f_2 = 0.$$

Geometrically, this implies that the line defined in the plane by the equation $L = 0$ goes through the point $\Phi(s:t) \in \mathcal{C}$.

For any integer $\nu \geqslant 0$, it is straightforward to compute a basis $L_1, \ldots, L_{r_\nu}$ of the vector space of moving lines of degree ν following Φ by solving a simple linear system. We define the matrix $\mathbb{M}_\nu(\Phi)$, or simply $\mathbb{M}_\nu$, as the matrix whose columns are filled with the coefficients of the moving lines L_j with respect to the variables s,t. More precisely, $\mathbb{M}_\nu$ is defined by the matrix equality

$$(L_1 \; L_2 \; \cdots \; L_{r_\nu}) = (s^\nu \; s^{\nu-1}t \; \cdots \; t^\nu) \cdot \mathbb{M}_\nu. \tag{2.2}$$

It is of size $(\nu+1) \times r_\nu$ and its entries are linear forms in $k[x_0,x_1,x_2]$. Therefore, it has sense to evaluate the matrix $\mathbb{M}_\nu$ at a point $p \in \mathbb{P}^2$, which we denote by $\mathbb{M}_\nu(p)$.

Proposition 2.1.1. *For all integer $\nu \geqslant d-1$ we have $r_\nu \geqslant \nu+1$ and*

$$\operatorname{rank} \mathbb{M}_\nu(p) < \nu+1 \quad \Longleftrightarrow \quad p \in \mathcal{C}.$$

In addition, $r_{d-1} = d$ and $r_\nu > \nu+1$ if $\nu \geqslant d$.

Proof. See [11, §2] and [73]. □

Thus, Proposition 2.1.1 shows that the matrices $\mathbb{M}_\nu$ are implicit representations of the curve $\mathcal{C}$ for all $\nu \geqslant d-1$, in the sense that they allow to discriminate the points $p \in \mathbb{P}^2$ that belong to the curve $\mathcal{C}$. Introduced first in [73] as the method of moving lines, the matrix $\mathbb{M}_{d-1}$ is a particular member in the family of matrices $\mathbb{M}_\nu$,

$\nu \geqslant d-1$: it is a square matrix whose determinant gives an implicit equation of the curve $\mathcal{C}$ raised to the power the degree of Φ [11, 31]. By the degree of Φ we mean the number of pre-images of a general point on $\mathcal{C}$ via Φ and over the algebraic closure $\overline{k}$ of k. In other words, this is nothing but the number of times the curve $\mathcal{C}$ is traced by the parameterization Φ over $\overline{k}$.

μ-basis

In the foundational paper [31], among other results the authors show that the matrices $\mathbb{M}_\nu$ exhibit a specific structure by introducing the concept of μ-basis.

Proposition 2.1.2. *There exists two moving lines p_1 and p_2 following Φ such that any moving line L following Φ can be written as*

$$L = h_1 p_1 + h_2 p_2,$$

where h_1 and h_2 are homogeneous polynomials in $k[s,t]$. Such a couple of moving lines p_1, p_2 is a called a μ-basis of the parameterization Φ. In addition, the degrees μ_1 and μ_2 of the moving lines p_1 and p_2 only depend on Φ and are such that $\mu_1 + \mu_2 = d$.

Proof. See for instance [26] and [31]. □

As a consequence of this proposition, the vector space of moving lines we used to define the matrices $\mathbb{M}_\nu(\Phi)$ have a simple description. More precisely, for any integer ν we have

$$\langle L_1, \ldots, L_{r_\nu} \rangle = \langle s^{\nu-\mu_1} p_1, s^{\nu-\mu_1-1} t p_1, \ldots, t^{\nu-\mu_1} p_1, s^{\nu-\mu_2} p_2, \ldots, t^{\nu-\mu_2} p_2 \rangle$$

where it is understood that the multiples of p_1, respectively p_2, disappear if $\nu < \mu_1$, respectively $\nu < \mu_2$. It follows that

$$r_\nu = \max(0, \nu - \mu_1 + 1) + \max(0, \nu - \mu_2 + 1).$$

Moreover, written in these special bases the matrices $\mathbb{M}_\nu$ exhibit a Sylvester-like block structure. In particular, in these bases the matrix $\mathbb{M}_{d-1}$ is nothing but the classical Sylvester matrix associated to the polynomials p_1 and p_2 with respect to the homogeneous variables s, t, denoted $\mathrm{Syl}(p_1, p_2)$. Thus, we recover the property that the resultant of these two polynomials, which is defined as the determinant of $\mathrm{Syl}(p_1, p_2)$, is equal to an implicit equation of $\mathcal{C}$ raised to the power the degree of Φ.

Several methods have been proposed to compute a μ-basis. The first type of methods starts from a generating collection of moving lines following Φ, namely the obvious moving lines of degree d of the form

$$f_i(s,t)x_j - f_j(s,t)x_i, \quad 0 \leqslant i < j \leqslant 2, \tag{2.3}$$

and uses various reductions to reach iteratively a μ-basis by means of linear algebra algorithms; see e.g. [26, 51]. Another type of methods arise from the computation of normal forms of matrices over a principal ideal domain, typically the computation of a Popov form; see e.g. [67, 85]. So far, these latter methods exhibit the best theoretical complexity.

The matrix $\mathbb{M}_{d-1}$ is the smallest matrix that is an implicit representation of the curve in the family of matrices $\mathbb{M}_\nu$. For a general parameterization Φ, the implicit equation of the curve is a degree d homogeneous polynomial equation in $k[x_0, x_1, x_2]$.

Therefore, the matrices $\mathbb{M}_\nu$ with $\nu \leqslant d-2$ cannot yield an implicit representation of $\mathcal{C}$ because their entries are linear forms in $k[x_0, x_1, x_2]$. As a consequence, to obtain more compact matrices it is necessary to introduce high-order extensions of the moving lines. Having in mind the correspondence between $\mathbb{M}_{d-1}$ and the Sylvester matrix $\mathrm{Syl}(p_1, p_2)$, the well-know family of (hybrid) Bézout matrices of p_1, p_2, which provides more compact matrices for the resultant, suggests to introduce quadratic forms in some entries of the matrices we consider.

Moving conics

As we call a moving line an equation of a line in the plane that moves as the parameter $(s : t) \in \mathbb{P}^1$ varies, we call a *moving conic* an equation of a conic in the plane whose coefficients depend on the parameter $(s : t) \in \mathbb{P}^1$. More concretely, a *moving conic* of degree $\nu \in \mathbb{N}$ is a polynomial of the form

$$\begin{aligned} Q(s,t;x_0,x_1,x_2) = g_{0,0}(s,t)x_0^2 + g_{0,1}(s,t)x_0x_1 + \\ g_{0,2}(s,t)x_0x_2 + g_{1,1}(s,t)x_1^2 + g_{1,2}(s,t)x_1x_2 + g_{2,2}(s,t)x_2^2 \end{aligned}$$

where the polynomials $g_{i,j}(s,t)$ are homogeneous polynomials of degree ν in $k[s,t]$. In addition, this moving conic is said to follow the parameterization Φ if

$$Q(s,t;f_0,f_1,f_2) = \sum_{0\leqslant i\leqslant j\leqslant 2} g_{i,j}(s,t)f_i(s,t)f_j(s,t) = 0.$$

Similarly to moving lines, this latter condition means geometrically that the conic defined in the plane by the polynomial Q goes through the point $\Phi(s : t) \in \mathcal{C}$.

We can consider the vector space of moving conics following the parameterization Φ of degree ν and, similarly to what we did with moving lines, build a coefficient matrix from them. However, such a matrix is useless in general because its entries are exclusively quadratic forms in $k[x_0, x_1, x_2]$ and hence the determinants of its minors are always polynomials of even degree. Having in mind the (hybrid) Bézout matrix that we previously mentioned, a better option is to combine both moving lines and moving conics in a same coefficient matrix. We proceed as follows.

Pick an integer $\nu \geqslant 0$. As explained in §2.1.1, choosing a basis of the vector space of moving lines following Φ of degree ν, denoted $\langle L_1, \ldots, L_{r_\nu}\rangle$, one can build the matrix $\mathbb{M}_\nu$. Now, one can consider the vector space W_ν of moving conics following Φ of degree ν. As it turns out, each moving lines L_j gives the three moving conics x_0L_j, x_1L_j and x_2L_j that all follow the parameterization Φ. Therefore, these $3r_\nu$ moving conics obtained from the moving lines, generate a sub-vector space V_ν of W_ν. By solving a linear system and computing a nullspace, one can compute a basis of the quotient vector space W_ν/V_ν that we denote by $\langle Q_1, \ldots, Q_{c_\nu}\rangle$. Then, we define the matrix $\mathbb{MQ}_\nu(\Phi)$, or simply $\mathbb{MQ}_\nu$, as the matrix satisfying to the equality

$$(L_1\ L_2\ \cdots\ L_{r_\nu}\ Q_1\ \cdots\ Q_{c_\nu}) = (s^\nu\ s^{\nu-1}t\ \cdots\ t^\nu)\cdot \mathbb{MQ}_\nu. \tag{2.4}$$

It is a matrix of size $(\nu+1)\times(r_\nu+c_\nu)$. By definition, its first r_ν columns is simply the matrix $\mathbb{M}_\nu$ whose entries are linear forms in $k[x_0, x_1, x_2]$, and its last c_ν columns are built from moving conics, so its entries are quadratic forms in $k[x_0, x_1, x_2]$.

We recall that μ_1 and μ_2 denote the degrees of a μ-basis of Φ. Without loss of generality we assume that $\mu_1 \leqslant \mu_2$.

Proposition 2.1.3. *If $\nu \geqslant \mu_2 - 1$ then $r_\nu + c_\nu \geqslant \nu + 1$ and*

$$\operatorname{rank} \mathbb{MQ}_\nu(p) < \nu + 1 \iff p \in \mathcal{C}.$$

In addition,

- *if $\mu_2 - 1 \leqslant \nu \leqslant d - 1$ then $r_\nu = 2(\nu+1) - d$, $c_\nu = d - 1 - \nu$ and the matrix $\mathbb{MQ}_\nu$ is a square matrix whose determinant is an implicit equation of $\mathcal{C}$, raised to the power the degree of Φ,*
- *if $\nu \geqslant d - 1$ then $c_\nu = 0$ and $\mathbb{MQ}_\nu = \mathbb{M}_\nu$.*

Proof. The proof can be done via an identification with the classical Sylvester and hybrid Bézout matrices, relying on their well-known properties. Indeed, it is a classical result that their determinants are all equal to the resultant of a μ-basis (see [35]) and that this latter is equal to an implicit equation of the parameterized curve $\mathcal{C}$ (raised to the power the degree of the corresponding parameterization). These results will be recovered in the next section §2.1.1 by interpreting the matrices $\mathbb{MQ}_\nu$ as resultant matrices. See also [74]. □

In the case where $\mu_1 = \mu_2 = h$, hence $d = 2h$, the matrix $\mathbb{MQ}_{h-1}$ is a $h \times h$-matrix whose entries are all quadratic forms, and whose determinant is an implicit equation of $\mathcal{C}$, raised to the power the degree of Φ. This is the only setting where such a fully quadratic matrix appears in the family of matrices of moving lines and conics. Notice that a general curve Φ such that $d = 2h$ satisfies to $\mu_1 = \mu_2$ (see [26]).

Sylvester forms

We already mentioned that the definition of the family of matrices $\mathbb{MQ}_\nu$ is inspired by the more classical family of (hybrid) Bézout matrices of a μ-basis p_1, p_2 of Φ. In what follows, we make explicit this comparison and exhibit in the same time a structure for the matrices $\mathbb{MQ}_\nu$. For that purpose we need to introduce the Sylvester forms.

Let p_1, p_2 be a μ-basis of the parameterization Φ and denote by $\mu_1 \leqslant \mu_2$ their respective degrees. We recall that $\mu_1 + \mu_2 = d$. Let $\alpha := (\alpha_1, \alpha_2)$ be any couple of non-negative integers such that $|\alpha| := \alpha_1 + \alpha_2 \leqslant \mu_1 - 1$. Since p_1 and p_2 are homogeneous polynomials in the variables s, t, one can decompose them as

$$\begin{aligned} p_1 &= s^{\alpha_1+1} h_{1,1} + t^{\alpha_2+1} h_{1,2}, \\ p_2 &= s^{\alpha_1+1} h_{2,1} + t^{\alpha_2+1} h_{2,2}, \end{aligned}$$

where $h_{i,j}(s, t; x_0, x_1, x_2)$ are homogeneous polynomials of degree $\mu_i - \alpha_j - 1$ with respect to the variables s, t and linear forms with respect to the variables x_0, x_1, x_2. Then, we define the polynomial

$$\operatorname{syl}_\alpha(p_1, p_2) := \det \begin{pmatrix} h_{1,1} & h_{1,2} \\ h_{2,1} & h_{2,2} \end{pmatrix}$$

and call it a *Sylvester form* of p_1, p_2.

Lemma 2.1.1. *For any α such that $|\alpha| \leqslant \mu_1 - 1$, the Sylvester form $\operatorname{syl}_\alpha(p_1, p_2)$ is a moving conic of degree $d - 2 - |\alpha|$ following the parameterization Φ. Moreover, it is independent of the choice of the polynomials $h_{i,j}$ modulo the μ-basis p_1, p_2, equivalently modulo the vector space of moving conics $V_{d-2-|\alpha|}$.*

Proof. The first assertion follows by construction and by the Cramer's rules for solving a linear system. For the rest, we refer to [55, §3.10]. □

It turns out that the Sylvester forms generate all the moving conics following Φ of degree greater or equal to $\mu_2 - 1$. Taking again the notation of §2.1.1, here is the precise result.

Proposition 2.1.4. *Let ν be an integer such that $\mu_2 - 1 \leqslant \nu \leqslant d-2$. Then the set of $d-1-\nu$ Sylvester forms*

$$\{\mathrm{syl}_\alpha(p_1,p_2)\}_{|\alpha|=d-2-\nu} = \left\{\mathrm{syl}_{(d-2-\nu,0)}(p_1,p_2),\ldots,\mathrm{syl}_{(0,d-2-\nu)}(p_1,p_2)\right\}$$

form a basis of the quotient vector space W_ν/V_ν of moving conics of degree ν following Φ and not generated from their corresponding moving lines, so that we have $c_\nu = d-1-\nu$. In addition, $W_{d-1} = V_{d-1}$ and hence $c_{d-1} = 0$.

Proof. These results follows from a duality property that we study in depth for general space curves in §2.3. □

As a consequence of this proposition, the construction of the matrices $\mathbb{MQ}_\nu$, $\nu \geqslant \mu_2 - 1$, following (2.1) can be done with more specific choices of the bases of moving lines and moving conics of degree ν. As we already used in §2.1.1, the space of moving lines can be chosen such that

$$\langle L_1,\ldots L_{r_\nu}\rangle = \langle s^{\nu-\mu_1}p_1, s^{\nu-\mu_1-1}tp_1,\ldots,t^{\nu-\mu_1}p_1, s^{\nu-\mu_2}p_2,\ldots,t^{\nu-\mu_2}p_2\rangle.$$

Moreover, by Proposition 2.1.4 the space of moving conics can be chosen as

$$\langle Q_1,\ldots Q_{c_\nu}\rangle = \langle \mathrm{syl}_{(d-2-\nu,0)}(p_1,p_2), \mathrm{syl}_{(d-3-\nu,1)}(p_1,p_2),\ldots,\mathrm{syl}_{(0,d-2-\nu)}(p_1,p_2)\rangle.$$

In this way, the matrix $\mathbb{MQ}_\nu$, $\nu \geqslant \mu_2 - 1$, exhibits a very particular structure: its first block of $r_\nu = 2(\nu+1) - d$ columns is the matrix $\mathbb{M}_\nu$, which is a Sylvester block built from the μ-basis p_1, p_2, and each of its last $c_\nu = d-1-\nu$ columns are filled with Sylvester forms of p_1 and p_2. This interpretation of the matrices $\mathbb{MQ}_\nu$, $\nu \geqslant \mu_2 - 1$, allows us to identify them with the family of (hybrid) Bézout matrices that are precisely defined in this way in the literature (see e.g. [35, 74]). The determinant of these Bézout matrices is known to be equal to the resultant of the μ-basis p_1, p_2 (see [55]). Therefore, we obtain the main property of these square matrices $\mathbb{MQ}_\nu$, $\mu_2 - 1 \leqslant \nu \leqslant d-1$: their determinants are all equal to an implicit equation of the curve $\mathcal{C}$, raised to the power the degree of Φ, as stated in Proposition 2.1.3.

In summary, the family of matrices $\mathbb{MQ}_\nu(\Phi)$, $\nu \geqslant \mu_2 - 1$, gives implicit matrix representations of the rational curve $\mathcal{C}$. It is an extension of the family of matrices $\mathbb{M}_\nu(\Phi)$, $\nu \geqslant d-1$ with more compact matrices obtained by introducing moving conics. The more compact matrix, namely $\mathbb{MQ}_{\mu_2-1}$, is made of a Sylvester block built from the polynomial p_1, possibly empty if $\mu_1 = \mu_2$, and then filled by columns with Sylvester forms.

In the next section, we will generalize the above results to the case of rational curves in arbitrary dimension. The family of matrices $\mathbb{M}_\nu(\Phi)$ built solely with moving lines, i.e. such that $\nu \geqslant d-1$, has already been extended to this setting in [16]; we will review it briefly. One of the main contribution in this thesis is the generalization of the matrices built with moving conics, i.e. the matrices $\mathbb{MQ}_\nu(\Phi)$ such that $\mu_2 - 1 \leqslant \nu \leqslant d-2$ to the case of rational curves in arbitrary dimension.

2.1.2 Maps from $\mathbb{P}^1$ to $\mathbb{P}^n$ with $n \geqslant 3$

Let $R := k[s,t]$ and $R' = k[x_0, \cdots, x_n]$ be a standard graded polynomial rings over a field k. Assume we are given a rational map

$$\begin{array}{rccl} \Phi: & \mathbb{P}^1_k & \to & \mathbb{P}^n_k \\ & (s:t) & \mapsto & (f_0(s,t) : \cdots : f_n(s,t)), \end{array} \tag{2.5}$$

where $f_0, \cdots, f_n$ are homogeneous polynomials in s and t of the same degree d greater or equal to 1. Assume that $f_0, \ldots, f_n$ do not have a common factor, then the image of Φ, denoted by $\mathfrak{I}m(\Phi)$, defines the curve $\mathcal{C}$ in $\mathbb{P}^n_k$. Let $I := (f_0, \cdots, f_n)$ be the ideal in R, $\mathfrak{m} := (s,t)$ be the irrelevant ideal of R. Let $S := k[s,t,x_0, \cdots, x_n]$ be the bi-graded polynomial ring over the field k with canonical grading $\deg(s) = \deg(t) = (1,0)$ and $\deg(x_i) = (0,1)$ for $i = 0, \cdots n$.

Moving hyperplanes and μ-basis

As a straightforward generalization of the concept of moving lines described in §2.1.1 for plane curves, a *moving hyperplane* of degree $\nu \in \mathbb{N}$ is a polynomial of the form

$$H(s,t;x_0,\ldots,x_n) = g_0(s,t)x_0 + \cdots + g_n(s,t)x_n$$

where $g_0, \ldots, g_n$ are homogeneous polynomials in $k[s,t]$ of degree ν. Thus, for any point $(s_0 : t_0) \in \mathbb{P}^1_k$, $H(s_0,t_0;x_0,\ldots,x_n)$ can be interpreted as the defining equation of a hyperplane in $\mathbb{P}^n_k$ that moves when the point $(s_0 : t_0)$ varies in $\mathbb{P}^1_k$. The moving hyperplane H is said to *follow the parameterization* Φ if

$$H(s,t;f_0(s,t),\ldots,f_n(s,t)) = g_0f_0 + \cdots + g_nf_n = 0,$$

which means geometrically that this hyperplane of equation $H = 0$ goes through the point $\Phi(s:t) \in \mathcal{C}$.

For any integer ν, one can compute a basis $H_1, \ldots, H_{r_\nu}$ of the vector space (over k) of the moving hyperplanes of degree ν following Φ. Then, one can define a coefficient matrix $\mathbb{M}_\nu$ by means of the following equality:

$$\begin{pmatrix} s^\nu & s^{\nu-1}t & \cdots & t^\nu \end{pmatrix} \cdot \mathbb{M}_\nu = \begin{pmatrix} H_1 & \cdots & H_{r_\nu} \end{pmatrix}.$$

The matrix $\mathbb{M}_\nu$ is of size $(\nu+1) \times r_\nu$ and its entries are linear forms in $k[x_0,\ldots,x_n]$, so it makes sense to evaluate it at a point in $\mathbb{P}^n_k$. For instance, by definition we have that for all point $(s_0 : t_0) \in \mathbb{P}^1_k$ this matrix satisfies to

$$\begin{pmatrix} s_0^\nu & s_0^{\nu-1}t_0 & \cdots & t_0^\nu \end{pmatrix} \cdot \mathbb{M}_\nu(\Phi(s_0,t_0)) = \begin{pmatrix} 0 & \cdots & 0 \end{pmatrix}. \tag{2.6}$$

This property implies that for any integer ν and any point $p \in \mathcal{C}$ the cokernel (or left nullspace) of $\mathbb{M}_\nu(p)$ has positive dimension. Actually, one can show that if $\nu \geqslant d-1$ then $r_\nu > \nu+1$ and we have that

$$\operatorname{rank} \mathbb{M}_\nu(p) < \nu+1 \iff p \in \mathcal{C}$$

(see [11, §2],[73]). However, this first generalization of Proposition 2.1.1 can be improved, but in order to state it we first need to introduce the concept of μ-basis for a parameterized curve in $\mathbb{P}^n$, $n \geqslant 2$, that has been introduced in [31] and then extensively studied (see e.g. [77] and [52, §4]).

Proposition 2.1.5. *There exist n moving hyperplanes $p_1, \ldots, p_n$ following Φ such that any moving hyperplane H following Φ can be written in the form*

$$H = h_1 p_1 + h_2 p_2 \ldots + h_n p_n,$$

where $h_1, \ldots, h_n$ are homogeneous polynomials in $k[s,t]$. Such an n-tuple of moving hyperplanes $p_1, \cdots, p_n$ are called a μ-basis of the parameterization Φ. In addition, let $\mu_1, \ldots, \mu_n$ be the degrees of the polynomials $p_1, \ldots, p_n$ respectively and assume without loss of generality that $\mu_1 \leqslant \mu_2 \leqslant \ldots \leqslant \mu_n$. Then, the sequence $(\mu_1, \ldots, \mu_n)$ only depends on the parameterization Φ and $\sum_{i=1}^{n} \mu_i = d$.

Proof. Let Φ be a parameterization as in (2.5). By Hilbert-Burch Theorem [9, Theorem 1.4.16], the ideal $I = (f_0, \ldots, f_n)$ has a free resolution

$$0 \to \oplus_{i=1}^{n} k[s,t](-d-\mu_i) \xrightarrow{M} \oplus_{i=0}^{n} k[s,t](-d) \xrightarrow{[f_0 \cdots f_n]} I \to 0,$$

where $[f_0 \cdots f_n]$ is a row matrix and $M = (m_{ij})_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n}}$ is a $(n+1) \times n$-matrix of polynomials over $k[s,t]$ of degree at most d such that $[f_0 \cdots f_n] \cdot M = 0$. Then, $p_1, \ldots, p_n$ is a μ-basis of the parameterization Φ such that

$$p_j(s,t,x_0,\ldots,x_n) = \sum_{i=0}^{n} (s,t) x_j \in k[s,t,x_0,\ldots,x_n],$$

(see e.g. [77, §2] and [31, §5]). □

Coming back to the family of matrices $\mathbb{M}_\nu$, they have a Sylvester block structure inherited from the existence of μ-basis. In particular,

$$r_\nu = \sum_{i=1}^{n} \max(0, \nu - \mu_i + 1). \tag{2.7}$$

Moreover, we have the following generalization of Proposition 2.1.1.

Proposition 2.1.6. *For all integer $\nu \geqslant \mu_n + \mu_{n-1} - 1$ we have $r_\nu > \nu + 1$ and*

$$\operatorname{rank} \mathbb{M}_\nu(p) < \nu + 1 \iff p \in \mathcal{C}.$$

Proof. See [16]. □

As in the case of plane curves, the matrices $\mathbb{M}_\nu$ give implicit representations of the curve $\mathcal{C}$ for all ν above a certain threshold (observe that if $n = 2$ then $\mu_2 + \mu_1 - 1 = d - 1$). Indeed the point p on the curve $\mathcal{C}$ is characterized by the fact that the rank of such a matrix evaluated at p is not maximal. Compared to an implicit polynomial representation, this is much more efficient since only a single matrix is necessary. Moreover, these matrices allow to recover the pre-images of such points p and they are also adapted to numerical treatments by means of numerical linear algebra techniques (see [16, 18]). In what follows, we extend this family of matrices in order to obtain more compact matrices still providing an implicit representation of $\mathcal{C}$.

Defining ideal in $\mathbb{P}^n$

Let $J := (p_1, \cdots, p_n)$ be the ideal in S which is generated by all the moving planes following Φ, hence generated by the μ-basis of the ideal I such that $\deg_R(p_i) = \mu_i$

and $\deg_{R'}(p_i) = 1$ for $i = 1, \cdots, n$. Let $B := S/J$ be the quotient ring which is the symmetric algebra of I, denoted by $\mathrm{Sym}(I)$. Let $\_^{sat}$ and $(\_ :_S \mathfrak{m}^\infty)$ both denote the saturation by the irrelevant ideal $\mathfrak{m}$ in S. Without loss of generality, we can assume that f_i's, $i = 0, \cdots, n$ do not have a common factor (otherwise, the f_i's can be simplified by their common factor). Then, we deduce that the polynomials $p_1, \ldots, p_n$ have no common root in $\mathbb{P}^1_k$ as well, [16, Lemma 1]. Algebraically, this means that they form a regular sequence [41, Chapter 17] outside of $V(\mathfrak{m})$ in S. Then we have

$$J^{sat} := (J :_S \mathfrak{m}^\infty) = \{s \in S : \exists n \in \mathbb{N} \quad s\mathfrak{m}^n \subset J\},$$

where S/J^{sat} is the Rees algebra of I, denoted by $\mathrm{Rees}(I)$ (see §1.2). Moreover, J and J^{sat} are both bi-graded ideals of S with respect to the grading of S. Let's recall that by definition (see §1.1)

$$H^0_{\mathfrak{m}}(B) = \{b \in B : \exists n \in \mathbb{N} \quad b\mathfrak{m}^n = 0\} \simeq (J :_B \mathfrak{m}^\infty)/\simeq = J^{sat}/J. \tag{2.8}$$

The graph Γ_Φ of Φ (see §1.1) can be given as the zero locus of homogeneous polynomials in coordinates $x_0, \ldots, x_n$ on $\mathbb{P}^n_k$, whose coefficients are polynomials in s, t on $\mathbb{P}^1_k$. We have two canonical projections from Γ_Φ, first one is onto the first component, i.e. $\pi_1 : \Gamma_\Phi \to \mathbb{P}^1_k$, the second one is on the last component, i.e. $\pi_2 := \Gamma_\Phi \to \mathbb{P}^n_k$. In addition, we have the following diagram

$$\begin{array}{ccc} \Gamma_\Phi & \hookrightarrow & \mathbb{P}^1_k \times \mathbb{P}^n_k \\ {\scriptstyle \pi_1}\downarrow & \nearrow_{\pi_2} & \\ \mathbb{P}^1_k & \xrightarrow{\Phi} & \mathbb{P}^n_k \end{array} \tag{2.9}$$

Moreover $\pi_2(\Gamma_\Phi)$ can be interpreted as the set of points $(x_0 : \cdots : x_n)$ for which the polynomials defining Γ_Φ have non-trivial solutions in s and t, i.e. either s or t value is non-zero. We would like to eliminate $x_0, \ldots, x_n$, for that reason consider the projective elimination ideal $\mathcal{I}$ in [28, Chapter8, §5]

$$\begin{aligned} \mathcal{I} &:= \{P \in R' : \exists n \in \mathbb{N} \quad P\mathfrak{m}^n \subset J\} \subset R' \\ &= (J : m^\infty) \bigcap R' \\ &= J^{sat} \bigcap R' \text{ (see §1.1).} \end{aligned}$$

Here we notice that $H^0_{\mathfrak{m}}(B)_0$ is the projective elimination ideal $\mathcal{I}$.

We consider the kernel of the ring homomorphism

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

$\ker(h)$ which is the set of polynomials $P(x_0, \ldots, x_n)$ such that $P(x_0, \ldots, x_n) = 0$ is called *the defining ideal $\mathfrak{I}_\mathcal{C}$ of the curve $\mathcal{C}$*. It is an ideal of R'. In terms of algebraic varieties, we have

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

Since the sequence $p_1, \ldots, p_n$ defines a regular sequence outside of $V(\mathfrak{m})$, $\mathrm{Rees}(I)$ is projectively isomorphic to $\mathrm{Sym}(I)$ (see [14]). Moreover, the algebraic variety $\boldsymbol{V}$ defined by zero locus of the μ-basis

$$\boldsymbol{V} := \{(s : t) \times (x_0 : \cdots : x_n) : p_1 = \cdots = p_n = 0\} \subset \mathbb{P}^1_k \times \mathbb{P}^n_k$$

is the graph of the rational map Φ and $\pi_2(\boldsymbol{V}) = \mathcal{C} = V(\mathfrak{I}_{\mathcal{C}})$ (see [16]). Also, by [14, Corollary 3.8] the projective elimination ideal $\mathcal{I}$ and the defining ideal of the curve $\mathcal{C}$ are the same.

2.2 The method of moving quadrics

2.2.1 Moving quadrics

Definition 2.2.1. *A* moving quadric *of degree $\nu \in \mathbb{N}$ is defined to be a polynomial of the form*

$$Q(s,t;x_0,\ldots,x_n) = \sum_{0\leq i\leqslant j\leq n} q_{ij}(s,t)x_ix_j$$

where $q_{i,j}(s,t)$, $0 \leq i \leqslant j \leq n$, are $n(n+1)/2$ homogeneous polynomials in $k[s,t]$. In addition, a moving quadric is said to follow the parameterization Φ if

$$Q(s,t;\Phi_0(s,t),\ldots,\Phi_n(s,t)) = 0.$$

Hence the polynomial Q defines a *quadric* in space that moves with the parameter $(s:t) \in \mathbb{P}^1_k$ and that goes through the point $\Phi(s,t) \in \mathcal{C}$.

Choose an integer ν and let $\langle H_1,\ldots,H_{r_\nu}\rangle$ be a basis of the vector space of moving hyperplanes following Φ. We can consider the vector space W_ν of moving quadrics following Φ. Each moving hyperplane H_j of degree ν following Φ generates $n+1$ moving quadrics of the same degree ν, still following Φ, that are given by x_iH_j, $0 \leq i \leq n$. Observe that geometrically, such a moving quadric consists of the union of the moving hyperplane of equation $H_j = 0$ and the static hyperplane of equation $x_i = 0$. We denote by V_ν the sub-vector space of moving quadrics generated by these moving quadrics obtained from moving hyperplanes. Now, let $\langle Q_1,\ldots,Q_{c_\nu}\rangle$ be a basis of the quotient vector space W_ν/V_ν. Then,

Definition 2.2.2. *We define the matrix $\mathbb{MQ}_\nu(\Phi)$ by*

$$(H_1\ H_2\ \cdots\ H_{r_\nu}\ Q_1\ \cdots\ Q_{c_\nu}) = (s^\nu\ s^{\nu-1}t\ \cdots\ t^\nu)\cdot\mathbb{MQ}_\nu.$$

It is a matrix of size $(\nu+1)\times(r_\nu+c_\nu)$, r_ν being given by (2.7).

Observe that this definition encapsulates the definition of the similar matrices we considered in the case $n = 2$, §2.1.1. By definition, the first r_ν columns of $\mathbb{MQ}_\nu$ correspond to the matrix $\mathbb{M}_\nu$ introduced in §2.1.2 and its entries are linear forms in $k[x_0,\ldots,x_n]$. On the other hand, its last c_ν columns are built from moving quadrics and hence its corresponding entries are quadratic forms in $k[x_0,\ldots,x_n]$. The definition of the matrices $\mathbb{MQ}_\nu$ is translated into Algorithm 1.

Algorithm 1: Construction of the matrices $\mathbb{MQ}_\nu$

Input : A parameterization Φ of a curve as defined in (2.5) and an integer ν.

Output: The matrix $\mathbb{MQ}_\nu$.

1. Compute a basis of the moving hyperplanes following Φ of degree ν and build the matrix $\mathbb{M}_\nu$.
2. Compute a basis $\langle Q_1, \ldots, Q_{c_\nu} \rangle$ of the vector space $W_\nu \,/\, V_\nu$; its k-th element is of the form
$$Q_k = \sum_{0 \leqslant i \leqslant j \leqslant n} \sum_{l=0}^{\nu} c_{k,l,i,j} s^{\nu-l} t^l x_i x_j$$
3. Define the matrices $M_{i,j} = (c_{k,l,i,j})_{l,k}$ and the matrix $\mathbb{Q}_\nu = \sum_{0 \leqslant i \leqslant j \leqslant n} M_{i,j} x_i x_j$.
4. Return the concatenated matrix
$$\mathbb{MQ}_\nu = \left(\begin{array}{c|c} \mathbb{M}_\nu & \mathbb{Q}_\nu \end{array} \right).$$

We recall that the sequence of increasing integers $\mu_1 \leqslant \mu_2 \leqslant \ldots \leqslant \mu_n$ denote the degrees of a μ-basis of Φ. Here is our first main result.

Theorem 2.2.1. *Assume that $\nu \geqslant \mu_n - 1$. Then, $r_\nu + c_\nu \geqslant \nu + 1$ and the degree of the fiber at $p \in \mathcal{C}$, i.e. $\deg(\pi_2^{-1}(p))$ where π_2 is as in (2.9), is equal to corank of $\mathbb{MQ}_\nu(p)$. In particular,*

$$\operatorname{rank} \mathbb{MQ}_\nu(p) < \nu + 1 \iff p \in \mathcal{C}.$$

Moreover, we have that

$$c_\nu = \sum_{1 \leqslant i < j \leqslant n} \max(0, \mu_i + \mu_j - 1 - \nu).$$

Also, if $\nu \geqslant \mu_n + \mu_{n-1} - 1$ then $c_\nu = 0$ and it follows that $\mathbb{MQ}_\nu = \mathbb{M}_\nu$.

Proof. See §2.3. □

Now, we discuss the shape of this matrix for some specific values of the degrees of the μ-basis. We emphasize that unlike in the case of plane curves, the matrices $\mathbb{MQ}_\nu$ will never be square matrices for space curves because a space curve cannot be defined by a single equation over an algebraically closed field.

In the family of matrices $\mathbb{MQ}_\nu$, $\nu \geqslant \mu_n - 1$, the matrix $\mathbb{MQ}_{\mu_n - 1}$ is evidently the one with the smallest number of rows. Moreover, the smallest possible value for the integer μ_n is $\lceil d/n \rceil$ because of the equality $\sum_{i=1}^n \mu_i = d$. It corresponds to the situation where the μ_i's are evenly distributed. It turns out that this balanced situation is the generic one when k is an algebraic closed field: fixing a degree d and picking n random homogeneous polynomials in (s,t) of degree d, $f_0, \ldots, f_n$ using a dense distribution of the coefficients such as Gaussian distribution, the degrees of its μ-basis are evenly distributed with probability 1 (see [34, Theorem 1.2] for the case $n = 2$ and [31, Section 3, Theorem 1] for a proof that generalizes to arbitrary dimension $n \geqslant 2$).

Here are some further specific settings:

- $\mu_1 = 0$: An element of degree 0 in the μ-basis corresponds to a (non-moving) hyperplane containing the curve. In this situation, we have $\mu_2 + \ldots + \mu_n = d$ and the problem is reduced to examining a curve in $\mathbb{P}^{n-1}$ whose μ-basis is $(p_2, \ldots, p_n)$.
- $\mu_1 = \mu_2 = 1$: In this situation, the curve is contained in a (non-moving) quadric whose equation is given by the resultant of p_1 and p_2.
- $\mu_i = d/n$ for all i: In this case, the degree d is a multiple of n and the matrix $\mathbb{MQ}_{d/n-1}$ is purely quadratic since there is no moving hyperplane of degree $d/n-1$ following the parameterization.

2.2.2 Sylvester forms

For any couple of integers $1 \leqslant i < j \leqslant n$ and any $\alpha = (\alpha_1, \alpha_2)$ such that $|\alpha| \leqslant \mu_i - 1$, one can consider the Sylvester form $\mathrm{syl}_\alpha(p_i, p_j)$, as defined in §2.1.1. Similarly to Lemma 2.1.1, one can show that it is a moving quadric following Φ of degree $\mu_i + \mu_j - 2 - |\alpha|$ that is independent of the choice of decomposition modulo the polynomials p_i, p_j.

Now, for any integer ν consider the vector space S_ν that is generated by all the Sylvester forms of degree ν, i.e.

$$\mathrm{S}_\nu = \langle \mathrm{syl}_\alpha(p_i, p_j) \text{ such that } \ 1 \leq i < j \leq n \text{ and } |\alpha| = \mu_i + \mu_j - 2 - \nu \rangle .$$

Taking again the notation of §2.2.1, it is a sub-vector space of the space W_ν of moving quadrics of degree ν following Φ. Here is our second main result.

Theorem 2.2.2. *If $\nu \geq \mu_n - 1$ then $W_\nu = V_\nu \oplus \mathrm{S}_\nu$. In other words, the moving quadrics of degree ν following Φ are generated by the moving hyperplanes of degree ν following Φ and by the Sylvester forms of degree ν. Moreover, these latter Sylvester forms are linearly independent and hence*

$$\dim \mathrm{S}_\nu = c_\nu = \sum_{1 \leqslant i < j \leqslant n} \max(0, \mu_i + \mu_j - \nu - 1).$$

Proof. See §2.3. □

Compared to Algorithm 1 described in §2.2.1, this theorem shows that the matrices $\mathbb{MQ}_\nu$ can be computed in *closed form* in terms of the polynomials $p_1, \ldots, p_n$ defining a μ-basis of Φ. We notice that, as far as we know, there is no known method that allows to compute the degrees $\mu_1, \ldots, \mu_n$, or even the degree μ_n, efficiently without actually computing a μ-basis. So, assuming the a μ-basis is computed, Theorem 2.2.2 gives an optimal method to build an implicit matrix representation of the curve $\mathcal{C}$ since it shows that the matrices $\mathbb{MQ}_\nu$ can be computed essentially at the cost of computing a μ-basis. This is described with more details in Algorithm 2 for the smallest matrix $\mathbb{MQ}_{\mu_n - 1}$. Of course, a similar algorithm can be used to build the matrix $\mathbb{MQ}_\nu$ for any integer $\nu \geqslant \mu_n - 1$, but we prefer to focus on the smallest matrix which is the more useful in practice.

Algorithm 2: Construction of $\mathbb{MQ}_{\mu_n-1}$

Input : A parametric curve Φ defined by (2.5)
Output: The matrix $\mathbb{MQ}_{\mu_n-1}$.

1. Compute a μ-basis $(p_1, \dots, p_n)$ of Φ. Let μ_i be the degree of p_i and assume that $\mu_1 \leqslant \cdots \leqslant \mu_n$.

2. Let $\mathcal{B}$ be a basis of the polynomial of degree $\mu_n - 1$, for instance
$$\mathcal{B} := \{s^{\mu_n-1}, s^{\mu_n-2}t, \dots, t^{\mu_n-1}\}.$$

3. Initialize the matrix $\mathbb{MQ}_{\mu_n-1}$ to the empty matrix. We build it by successively adding columns as follows.

4. For i from 1 to $n-1$ add a block of $\mu_n - \mu_i$ columns to the matrix $\mathbb{MQ}_{\mu_n-1}$ corresponding to the coefficients of the polynomials
$$\{s^{\mu_n-\mu_i-1}p_i, s^{\mu_n-\mu_i-2}tp_i, \dots, t^{\mu_n-\mu_i-1}p_i\}$$
with respect to the polynomial basis $\mathcal{B}$.

5. For i from 1 to $n-1$ do
for j from $i+1$ to n do
if $\nu_{i,j} := \mu_i + \mu_j - \mu_n - 1 \geqslant 0$ then add a block of $\nu_{i,j}+1$ columns to the matrix $\mathbb{MQ}_{\mu_n-1}$ corresponding to the coefficients of the Sylvester forms
$$\{\mathrm{syl}_\alpha(p_i, p_j) : |\alpha| = \nu_{i,j}\}$$
with respect to the polynomial basis $\mathcal{B}$.

6. Return the matrix $\mathbb{MQ}_{\mu_n-1}$.

2.3 Proofs of the main theorems

In this section, we prove Theorem 2.2.1 and Theorem 2.2.2.

With the notation of §2.1.2, the ideals J and J^{sat} are both bi-graded ideals. They have a grading with respect to the variables s, t and with respect to the variables $x_0, \dots, x_n$. We denote by J_ν and $(J^{sat})_\nu$ the graded slices of degree $\nu \in \mathbb{N}$ with respect to the variables s, t. They are $k[x_0, \dots, x_n]$-modules. For instance,
$$(J^{sat})_0 = J^{sat} \cap k[x_0, \dots, x_n] = \mathfrak{I}_\mathcal{C}.$$

2.3.1 Elimination and matrices

We have previously built matrices by columns with the coefficients with respect to s, t of some moving hyperplanes and quadrics following Φ of a given degree ν. Extending this approach, we could consider similar matrices built by columns with the coefficients of all the moving hypersurfaces following Φ in a given degree ν. Call these matrices $\mathbb{MH}_\nu$. Their entries are homogeneous polynomials in $k[x_0, \dots, x_n]$. They are defined up to a choice of basis of the polynomials in s, t of degree ν, and up to a choice of a set of generators of the set of moving hypersurfaces following Φ of degree ν.

Lemma 2.3.1. *For any integer $\nu \geqslant 0$ and any $p \in \mathbb{P}^n$,*

$$\operatorname{rank} \mathbb{MH}_\nu(p) < \nu + 1 \iff p \in \mathcal{C}.$$

Proof. Because of (2.8), we get that the annihilator $\operatorname{ann}_{R'}(S_\nu/(J^{sat})_\nu)$ is equal to the defining ideal $\mathfrak{I}_\mathcal{C}$ of the curve $\mathcal{C}$ for all integer $\nu \geqslant 0$ [16, §2.3]. Then, by classical properties of Fitting ideals [41, Chapter 20], we obtain that any free presentation of $S_\nu/(J^{sat})_\nu$, as a A-module, has the claimed property. As J^{sat} is generated by all the moving hypersurfaces following Φ, the conclusion follows. □

Although interesting, this property is not of practical interest because it is a difficult task to compute moving hypersurfaces in general. For instance in the extreme case $\nu = 0$, the matrix $\mathbb{MH}_0$ is a row matrix filled by columns with a generating set of $\mathfrak{I}_\mathcal{C}$. Nevertheless, with this interpretation, the main idea of the method of moving hyperplanes, resp. moving quadrics, is to tune the integer ν in order to have a control on the moving hypersurfaces that are needed. Typically, one may wonder for which integer ν the moving hyperplanes, resp. quadrics, generate all the moving hypersurfaces following Φ in this degree. Thus, Proposition 2.1.6 means that

$$\forall \nu \geqslant \mu_n + \mu_{n-1} - 1 \quad (J^{sat})_\nu = J_\nu, \tag{2.10}$$

i.e. above this threshold degree all the moving hypersurfaces following Φ are generated by the moving hyperplanes of the same degree following Φ. In the same vain, to prove Theorem 2.2.1, we have to show that

$$\forall \nu \geqslant \mu_n - 1 \quad (J^{sat})_\nu = (J^{sat}\langle 2\rangle)_\nu \tag{2.11}$$

where $J^{sat}\langle 2\rangle \subset J^{sat}$ denotes the ideal of S generated by all the moving planes and moving quadrics following Φ. More precisely $J^{sat}\langle \eta\rangle$ refers to the degree at most η over $k[x_0, \ldots, x_n]$ part of J^{sat}.

Let $K_\bullet$ be the Koszul complex (see Definition 1.3.2.) associated to the sequence $p_1, \cdots, p_n$ which generates the ideal J. Since J has the bi-grading structure, so does $K_\bullet$. In the sequel, $[\ \ ]$ and $\{\ \ \}$ denote the shifting with respect to $R = k[s,t]$ and $R' = k[x_0, \cdots, x_n]$ respectively. Let $S = R \otimes_k R'$. Then, $K_\bullet$ is given as follows

$$K_\bullet : K_n \xrightarrow{d_n} K_{n-1} \xrightarrow{d_{n-1}} \cdots \xrightarrow{d_2} K_1 \xrightarrow[(p_1,\cdots,p_n)]{d_1} K_0 = S \xrightarrow{d_0} 0,$$

where $K_m := \oplus_{1\leqslant i_1<\cdots<i_m\leqslant n} S[-\mu_{i_1} - \cdots - \mu_{i_m}]\{-m\}$. For instance,

$$K_1 := \oplus_{i=1}^n S[-\mu_i]\{-1\}.$$

Moreover, since the differential d_1 corresponds to row matrix $\begin{bmatrix} p_1 & \cdots & p_n \end{bmatrix}$ and we have

$$H_0(K_\bullet) = S/J.$$

Proposition 2.3.1. *We have the following isomorphism*

$$H_2(H^2_\mathfrak{m}(K_\bullet)) \cong H^0_\mathfrak{m}(B) = J^{sat}/J.$$

Proof. Consider the double complex $\mathscr{C}^\bullet_\mathfrak{m}(K_\bullet)$, where $\mathscr{C}^\bullet_\mathfrak{m}$ denotes the Čech complex with respect to $\mathfrak{m}$. The column filtered spectral sequences of $\mathscr{C}^\bullet_\mathfrak{m}(K_\bullet)$ stabilizes in the

second sheet as follows

$$\begin{array}{ccccc} H^0_{\mathfrak{m}}(H_n(K_\bullet)) & \cdots & H^0_{\mathfrak{m}}(H_2(K_\bullet)) & H^0_{\mathfrak{m}}(H_1(K_\bullet)) & H^0_{\mathfrak{m}}(H_0(K_\bullet)) \\ 0 & \cdots & 0 & 0 & H^1_{\mathfrak{m}}(H_0(K_\bullet)) \\ 0 & \cdots & 0 & 0 & H^2_{\mathfrak{m}}(H_0(K_\bullet)) \end{array}$$

The modules $H^i_{\mathfrak{m}}(H_j(K_\bullet)) = 0$ for $i > 0$ and $j > 0$, because of the fact that J annihilates the homology modules of $K_\bullet$ and the polynomials $p_1, \cdots, p_n$ form a regular sequence outside of $V(\mathfrak{m})$. On the other hand, the row filtered spectral sequence of $\mathscr{C}^\bullet_{\mathfrak{m}}(K_\bullet)$ stabilizes also at the second sheet.

$$\begin{array}{ccccc} 0 & \cdots & 0 & 0 & 0 \\ 0 & \cdots & 0 & 0 & 0 \\ H_n(H^2_{\mathfrak{m}}(K_\bullet)) & \cdots & H_2(H^2_{\mathfrak{m}}(K_\bullet)) & H_1(H^2_{\mathfrak{m}}(K_\bullet)) & H_0(H^2_{\mathfrak{m}}(K_\bullet)) \end{array}$$

Then by the comparison theorem of spectral sequences [83, p. 5.2.12], we have the desired isomorphism. □

We recall that the local cohomology modules of the ring S are defined to be

$$H^2_{\mathfrak{m}}(S) \cong R' \otimes_k \check{R}, \quad \check{R} := \frac{1}{st} k[s^{-1}t^{-1}], \tag{2.12}$$

and by Theorem 1.6.1 we have $H^i_{\mathfrak{m}}(S) = 0$ for all $i \neq 2$.

Corollary 2.3.1. *For all integers $\nu \geqslant \mu_n - 1$, we have the following exact sequence* $\oplus_{1\leqslant i<j<k\leqslant n}\check{R}_{\nu-\mu_i-\mu_j-\mu_k} \otimes_k R'\{-3\} \to$

$$\oplus_{1\leqslant i<j\leqslant n}\check{R}_{\nu-\mu_i-\mu_j} \otimes_k R'\{-2\} \to (J^{sat}/J)_\nu \to 0.$$

Proof. Consider the spectral sequences in the proof of the Proposition 2.3.1, in particular, last non-zero row of the first sheet of spectral sequences of $\mathscr{C}^\bullet_{\mathfrak{m}}(K_\bullet)$ with respect to the row filtration which is

$$H^2_{\mathfrak{m}}(K_n) \to \cdots \xrightarrow{d_3} H^2_{\mathfrak{m}}(K_2) \xrightarrow{d_2} H^2_{\mathfrak{m}}(K_1) \xrightarrow{d_1} H^2_{\mathfrak{m}}(K_0).$$

Then, $H_2(H^2_{\mathfrak{m}}(K_2)) = \ker d_2/\mathcal{I}m d_3$. Then by (2.12) and the fact that local cohomology commutes with direct sum, for all $\nu > \mu_n - 2$, we have

$$H^2_{\mathfrak{m}}(K_1)_\nu = H^2_{\mathfrak{m}}(\oplus_{i=1}^n S[-\mu_i]\{-1\})_\nu = \oplus_{i=1}^n \check{R}_{\nu-\mu_i} \otimes_k R'\{-1\} = 0.$$

If $H^2_{\mathfrak{m}}(K_1)_\nu = 0$, then $\ker(d_2)_\nu = H^2_{\mathfrak{m}}(K_2)_\nu$. Likewisely, for all $\nu > \mu_n - 2$, we have,

$$\begin{aligned} \ker(d_2)_\nu &= H^2_{\mathfrak{m}}(K_2)_\nu \\ &= H^2_{\mathfrak{m}}(\oplus_{1\leqslant i<j\leqslant n} S[-\mu_i-\mu_j]\{-2\})_\nu \\ &= \oplus_{1\leqslant i<j\leqslant n}\check{R}_{\nu-\mu_i-\mu_j} \otimes_k R'\{-2\}. \end{aligned}$$

Similarly we have,

$$\begin{aligned} H^2_{\mathfrak{m}}(K_3)_\nu &= H^2_{\mathfrak{m}}(\oplus_{1\leqslant i<j<k\leqslant n} S[-\mu_i-\mu_j-\mu_k]\{-3\})_\nu \\ &= \oplus_{1\leqslant i<j<k\leqslant n}\check{R}_{\nu-\mu_i-\mu_j-\mu_k} \otimes_k R'\{-3\}. \end{aligned}$$

Hence, for $\nu > \mu_n - 1$, we have the following exact sequence

$$\oplus_{1\leqslant i<j<k\leqslant n}\check{R}_{\nu-\mu_i-\mu_j-\mu_k}\otimes_k R'\{-3\}\to$$

$$\oplus_{1\leqslant i<j\leqslant n}\check{R}_{\nu-\mu_i-\mu_j}\otimes_k R'\{-2\}\to(J^{sat}/J)_\nu\to 0.$$

□

Proof of Theorem 2.2.1. Except the result on degree of fiber at point $p\in\mathcal{C}$, Theorem 2.2.1 follows straightforwardly from Corollary 2.3.1. Indeed, it shows that $(J^{sat})_\nu$ is generated by moving quadrics modulo the moving hyperplanes, i.e. modulo J_ν, and that the number of minimal generators, i.e. the dimension of the vector space of moving quadrics modulo the vector space of moving hyperplanes both in degree ν, is precisely given by c_ν. In particular, if $\nu\geqslant\mu_n+\mu_{n-1}-1$ we get that $(J^{sat}/J)_\nu=0$, i.e. that $(J^{sat})_\nu=J_\nu$. Hence, if $\nu\geqslant\mu_n+\mu_{n-1}-1$, all the moving hypersurfaces are generated by the moving planes and we have $c_\nu=0$.

Now let's prove that the degree of the fiber at point $p\in\mathcal{C}$ is equal to corank of $\mathbb{MQ}_\nu(p)$. For this, for any point $p\in\mathbb{P}^n$ by the Grothendieck-Serre formula, we have the equality (see for instance [6, Proposition 4.26])

$$HP_{\pi_2^{-1}(p)}(\nu)=HF_{\pi_2^{-1}(p)}(\nu)-\sum_{i\geqslant 0}(-1)^iHF_{H^i_{\mathfrak{m}}(\pi_2^{-1}(p))}(\nu).$$

Proposition 2.3.1 and Corollary 2.3.1 give us the vanishing of $H^0_{\mathfrak{m}}(S/J)$. It remains to look for the vanishing of $H^1_{\mathfrak{m}}(S/J^{sat}\langle 2\rangle)$. Using the spectral sequences associated to the double complex $\mathscr{C}^\bullet_{\mathfrak{m}}(K_\bullet)$ where $K_\bullet$ is the Koszul complex of a μ-basis of Φ, (given in Proof of Proposition 2.3.1), $H^2_{\mathfrak{m}}(H_1(K_1))\simeq H^1_{\mathfrak{m}}(B)$. We have already seen that for all $\nu>\mu_n-2$,

$$H^2_{\mathfrak{m}}(K_1)_\nu=H^2_{\mathfrak{m}}(\oplus_{i=1}^n S[-\mu_i]\{-1\})_\nu=\oplus_{i=1}^n\check{R}_{\nu-\mu_i}\otimes_k R'\{-1\}=0.$$

Let's consider the cohomology long exact sequences obtained by the short exact sequence

$$0\to J^{sat}\langle 2\rangle/J\to S/J\to S/J^{sat}\langle 2\rangle\to 0.$$

Hence, we have

$$\cdots\to H^1_{\mathfrak{m}}(S/J)_\nu\to H^1_{\mathfrak{m}}(S/J^{sat}\langle 2\rangle)_\nu\to H^2_{\mathfrak{m}}(J^{sat}\langle 2\rangle/J)_\nu\to\cdots$$

and $H^1_{\mathfrak{m}}(S/J^{sat}\langle 2\rangle)_\nu$ vanishes where $H^1_{\mathfrak{m}}(S/J)_\nu$ and $H^2_{\mathfrak{m}}(J^{sat}\langle 2\rangle/J)_\nu$ simultaneously vanish. By Proposition 2.3.1, we have $H^1_{\mathfrak{m}}(S/J)_\nu=0$ for all $\nu\geqslant\mu_n-1$. Then, $H^2_{\mathfrak{m}}(J^{sat}\langle 2\rangle/J)_\nu=0$, since $a_2(J)=a_2(J^{sat}\langle 2\rangle)$ (we refer the reader to §1.6 for the invariant a_i of local cohomology modules.). □

2.3.2 Proof of Theorem 2.2.2

The proof of Theorem 2.2.2 can be seen as a particular case of an explicit construction of duality isomorphism similar to the one we obtained in Proposition 2.3.1. Such an explicit construction already appeared in [56] and [33]. Now, we prove Theorem 2.2.2.

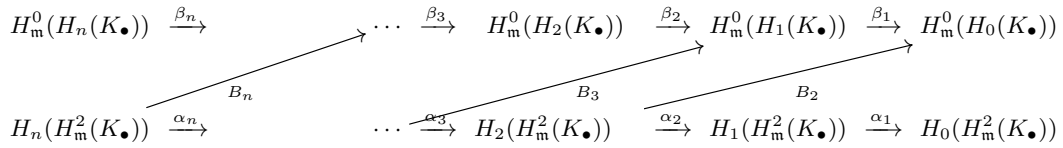
First, by Koszul self-duality (see §1.3), we have a graded isomorphism

$$H_i(H^2_{\mathfrak{m}}(K_\bullet))\simeq H_{n-i}(K_\bullet[\sum_{i=0}^n d-2])^*$$

where $(-)^*$ stands for the dual. Then, by the comparison theorem of the spectral sequences given in the proof of Proposition 2.3.1 we have the diagonal isomorphisms,

$$B_{i-2} := H_{n-i}(K_\bullet[\sum_{i=0}^{n} d-2])^* \xrightarrow{\sim} H^0_{\mathfrak{m}}(H_{i-2}(K_\bullet)), \text{ for } i=2,\dots,n,$$

which are known to be the Bezoutian maps given in [33, Theorem 1.3] as follows



Here, the α_i's and the β_i's are dual Koszul and Koszul differentials (see Definition 1.3.2 and Definition 1.3.3) respectively for $i=1,\dots,n$. We have also the following commutative diagram and the same diagram for the homologies, for all integer $i=1,\dots,n$

$$\begin{array}{ccc} K_{i-2} & \xrightarrow{\beta_i} & K_{i-3} \\ \uparrow{\scriptstyle B_i} & & \uparrow{\scriptstyle B_{i-1}} \\ K^*_{n-i} & \xrightarrow{\alpha_i} & K^*_{n-i+1}, \end{array}$$

which makes each cell of the above spectral sequences, $\beta_i \circ B_i = B_{i-1} \circ \alpha_i$, commutative.

In [56, Section 3] the generalized Morley form gives following explicit construction of the isomorphism denoted by B_n

$$B_n := 1 \mapsto \sum_{\substack{\sigma\in\mathcal{S}_n \text{ such that} \\ \sigma(1)<\sigma(2), \\ \sigma(3)<\ldots<\sigma(n)}} \operatorname{sign}(\sigma) \begin{vmatrix} p_{\sigma(1),1} & p_{\sigma(1),2} \\ p_{\sigma(2),1} & p_{\sigma(2),2} \end{vmatrix} e_{\sigma(3)} \wedge \cdots \wedge e_\sigma(n).$$

where $p_i(s:t) = s\dot{p}_{i,0}(s,t) + t\dot{p}_{i,1}(s,1)$ for $i=1,\dots,n$. Assume $e^*_{\sigma(1)} \wedge \cdots \wedge e^*_{\sigma(i)}$ be an element of K^*_i, then we have

$$B_i := (e^*_{\sigma(1)} \wedge \cdots \wedge e^*_{\sigma(i)}) \mapsto \sum_{\substack{\sigma\in\mathcal{S}_n \text{ such that} \\ \sigma(i)<\sigma(i+1)<\sigma(i+2), \\ \sigma(i)<\sigma(i+3)<\ldots<\sigma(n)}} \operatorname{sign}(\sigma) \begin{vmatrix} p_{\sigma(i+1),1} & p_{\sigma(i+1),2} \\ p_{\sigma(i+2),1} & p_{\sigma(i+2),2} \end{vmatrix} e_{\sigma(i+3)} \wedge \cdots \wedge e_\sigma(n).$$

Thus, B_0 gives an explicit construction of the map in Proposition 2.3.1. Then, to obtain Theorem 2.2.2 one has to show that for all degree $\nu \geqslant \mu_n - 1$ the graded components of this Morley form coincide with Sylvester forms. This latter property follows from [55, Proposition 3.11.13]. □

2.3.3 Koszul syzygies

For the sake of completeness, we discuss the link with the obvious moving hyperplanes of the form (2.3) that are also called Koszul syzygies. Let us denote by J_K the ideal generated by these moving hyperplanes. We have $J_K \subset J \subset J^{sat}$. As the polynomials $f_0,\dots,f_n$ have no common root in $\mathbb{P}^1_k$, we know that these three ideals coincide in sufficiently high degrees. Here is a more precise result.

Proposition 2.3.2. *For all integers $\nu \geqslant d+\mu_n+\mu_{n-1}-1$ we have $(J_K)_\nu = J_\nu$.*

Proof. The quotient $J/J_{\mathcal{K}}$ is canonically identified with the first homology group H_1^f of the Koszul complex associated to the sequence $f_0, \ldots, f_n$ which is of the form

$$K_{n+1}^f \to \cdots \to K_2^f \xrightarrow{d_2} K_1^f \xrightarrow{d_1} K_0^f.$$

Indeed, the kernel of d_1 corresponds to the μ-basis of Φ and the image of d_2 identifies to the Koszul syzygies, i.e. syzygies of form $f_i x_j - x_i f_j$, for $0 \leqslant i, j \leqslant n$. Taking into account the shifts in the grading, we get the isomorphism $(H_1^f)_{\nu+d} \simeq (J/J_{\mathcal{K}})_\nu$ for all integer ν.

Now, consider the sequence

$$0 \to Z_2^f \hookrightarrow K_2^f \xrightarrow{d_2} K_1^f \xrightarrow{d_1} K_0^f$$

where $Z_2^f = \ker d_2$. Then, from the two spectral sequences associated to the double complex

$$0 \to \mathscr{C}_{\mathfrak{m}}^\bullet(Z_2^f) \hookrightarrow \mathscr{C}_{\mathfrak{m}}^\bullet(K_2^f) \xrightarrow{d_2} \mathscr{C}_{\mathfrak{m}}^\bullet(K_1^f) \xrightarrow{d_1} \mathscr{C}_{\mathfrak{m}}^\bullet(K_0^f),$$

we deduce that $(H_1^f)_\nu = 0$ for any integer ν such that $H_{\mathfrak{m}}^2(Z_2^f)_\nu = 0$.

The two modules Z_2^f and Z_1^f are free graded $k[s,t]$-modules. Consider the canonical map $\wedge^2 Z_1^f \to Z_2^f$. Since the f_i's have no common root in $\mathbb{P}_k^1$, we deduce that the kernel and the cokernel of this map are supported on $V(\mathfrak{m})$, and therefore it must be a graded isomorphism. To conclude, we notice that

$$Z_1^f \simeq \oplus_{i=1}^n k[s,t](-d-\mu_i),$$

and the claimed result follows by (2.12). □

2.3.4 Summary of our results

To summarize, we have built a family of matrices $\mathbb{MQ}_\nu$ that provides implicit matrix representations of a parameterized curve in arbitrary dimension for all $\nu \geqslant \mu_n - 1$, where μ_n is the highest degree of a polynomial in a μ-basis of the parameterization of this curve. They have the following shape:

- If $\mu_n - 1 \leqslant \nu \leqslant \mu_n + \mu_{n-1} - 2$, then $\mathbb{MQ}_\nu$ is filled with moving planes and moving quadrics. It is exclusively filled with moving quadrics if and only if $\nu = \mu_n - 1$ and $\mu_i = d/n$ for all $i = 1, \ldots, n$.
- If $\nu \geqslant \mu_n + \mu_{n-1} - 1$, then $\mathbb{MQ}_\nu$ is filled with moving planes, and it coincides with the family of matrices $\mathbb{M}_\nu$ introduced in [16].
- If $\nu \geqslant d + \mu_n + \mu_{n-1} - 1$, then $\mathbb{MQ}_\nu = \mathbb{M}_\nu$ can be filled from the obvious moving planes of the form (2.3) without relying on the computation of a μ-basis. This is an improvement of [16, Proposition 26].

Example 2.3.1. *Consider the following parameterization Φ of a curve $\mathcal{C}$ of degree 6:*

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

$$\begin{pmatrix} x_0 & 0 & x_1+3x_2+3x_3 & \frac{3}{2}x_3 & \frac{1}{2}x_3 & 0 \\ 0 & x_0 & -\frac{9}{2}x_3x_1+3x_2-\frac{3}{2}x_3 & -x_3 & \frac{1}{2}x_3 & \\ -8x_0+x_1 & -3x_0 & 2x_1-9x_3 & -x_1-6x_3 & x_2-x_3 & -x_3 \\ 3x_0+3x_1 & x_0+x_1 & 3x_1-3x_3 & 3x_1-3x_3 & 0 & x_2-x_3 \end{pmatrix}$$

FIGURE 1. Matrix $\mathbb{M}_3$ of moving hyperplanes corresponding to the space curve parameterization discussed in Example 2.3.1.

$$\begin{pmatrix} 2x_0x_1-x_2^2-6x_0x_2-3x_1x_2 & 2x_0x_1+6x_0z_2 & 2x_0z_2-3x_0x_3-x_1x_3 \\ -8x_0x_1+x_1^2+12x_0x_2+3x_1x_2 & 2x_0x_1-x_1^2-6x_0x_2-3x_1x_2 & -6x_0x_2+8x_0x_3+2x_1x_3 \\ x_0x_3 & 2x_1x_2+6x_2^2-5x_1x_3-3x_2x_3 & -x_1x_3-3x_2x_3 \\ 2x_0x_2-3x_0x_3-x_1x_3 & -2x_1x_2-6x_2^2+8x_1x_3 & 2x_1x_2+6x_2^2-5x_1x_3-3x_2x_3 \end{pmatrix}.$$

FIGURE 2. Matrix $\mathbb{MQ}_1$ of moving quadrics corresponding to the space curve parameterization discussed in Example 2.3.1.

The computation of a μ-basis of Φ gives

$$\begin{aligned} p_1 &= (s^2-3st+t^2)x+t^2y \\ p_2 &= (s^2-st+3t^2)y+(3s^2-3st-3t^2)z, \\ p_3 &= 2t^2z+(s^2-2st-2t^2)w, \end{aligned}$$

so that we have $\mu_1=\mu_2=\mu_3=2$.

This example is taken from [53, Example 3.7] where the authors introduce three quartic surfaces in order to get an implicit representation of the curve $\mathcal{C}$. The equations of these quartic surfaces are given by the resultant of p_1 and p_2, of p_1 and p_3, and of p_2 and p_3 with respect to the homogeneous variables s and t. Their intersection always contains the curve $\mathcal{C}$ but it may also contains some extraneous components. For instance, in this example the point $q=(1:1:1:1)\in\mathbb{P}^3$ is not on the curve $\mathcal{C}$, but it belongs to the intersection of these three quartic surfaces.

In [16, Example 8], this same parameterization is implicitized by means of the matrix of moving hyperplanes $\mathbb{M}_3$ ($\mu_2+\mu_3-1=3$), which is of size 4×6. This matrix is proved to always give an implicit representation of the curve $\mathcal{C}$. Indeed, its rank is equal to 4 after evaluation at the point q, showing that $q\notin\mathcal{C}$. It is printed in Figure 1.

Now, according to the new family of matrices we built in this chapter, the matrix of $\mathbb{MQ}_1$ ($\mu_3-1=1$) also provides an implicit representation of the curve $\mathcal{C}$. It is a matrix of size 2×6, more compact than $\mathbb{M}_3$, which is filled with the 6 Sylvester forms $\mathrm{syl}_{(1,0)}(p_i,p_j)$ and $\mathrm{syl}_{(0,1)}(p_i,p_j)$ for $1\leqslant i<j\leqslant 3$. It is printed in Figure 2.

2.4 Computational aspects

In this section, we report on some experiments on the computation of the family of matrices $\mathbb{MQ}_\nu$ we have introduced. In particular, we illustrate the gain we obtain with the smallest matrix $\mathbb{MQ}_{\mu_n-1}$ for deciding whether a point belongs to a parameterized curve.

2.4.1 Computation of the matrices

In this paragraph we report on the size and the computation time of some implicit matrix representations that are of particular interest, in the case $n = 3$. More precisely, we retain the following matrices:

- Moving hyperplane matrices: both $\mathbb{M}_{d-1}$, in order to avoid the computation of a μ-basis, and $\mathbb{M}_{\mu_n+\mu_{n-1}-1}$, in which case (the degrees of) a μ-basis must be computed, are considered.
- $\mathbb{MQ}_{\text{ker}}$: the matrix of moving planes and moving quadrics in degree $\mu_n - 1$, computed using kernel calculations by Algorithm 1.
- $\mathbb{MQ}_{\text{Syl}}$: the matrix of moving planes and moving quadrics in degree $\mu_n - 1$ are built in closed form from a μ-basis, by means of Algorithm 2.

The results are reported below. The algorithms have been implemented in SageMath and run using an Intel(R) Pentium(R) N3540 CPU @ 2.16GHz on a x64 machine with 4GB of RAM.

In Table 2.1, we give the computation time of a μ-basis and then our two options to build an optimal implicit matrix representation: a matrix fully composed of moving planes or a mixed matrix with moving planes and moving quadrics. For these two matrices, the computation time excludes the computation of the μ-basis, which is reported in the second column. It appears clearly that the matrix with moving quadrics is more expensive to build, because its entries require calculations.

Degree d and degrees $(\mu_i)_i$	**μ-basis**	$\mathbb{M}_{\mu_n+\mu_{n-1}-1}$	$\mathbb{MQ}_{\text{Syl}}$
5 $(2,3)$	230ms	5x5 57ms	3x3 417ms
10 $(5,5)$	343ms	10x10 168ms	5x5 1503ms
10 $(1,9)$	292ms	10x10 166ms	9x9 614ms
5 $(1,2,2)$	156ms	4x7 94ms	2x5 676ms
9 $(3,3,3)$	151ms	6x9 141ms	3x9 2194ms
9 $(1,4,4)$	292ms	8x15 268ms	4x9 1900ms
9 $(1,1,7)$	396ms	8x15 244ms	7x14 1132ms
15 $(5,5,5)$	281ms	10x15 332ms	5x15 5516ms
15 $(1,7,7)$	647ms	14x27 782ms	7x15 4663ms
15 $(1,1,13)$	1477ms	14x27 657ms	13x26 2810ms

Table 2.1: Computation time in milliseconds of a μ-basis and two typical implicit matrix representations built from the μ-basis.

In the Table 2.2, we assume that a μ-basis is unknown and then compare the computation time of the matrix $\mathbb{M}_{d-1}$, which does not require the computation of a μ-basis, with the computation time of the matrix $\mathbb{MQ}_{\mu_n-1}$ via our two algorithms, for which a μ-basis is computed. As expected, the faster matrix to compute is $\mathbb{M}_{d-1}$.

Degree d and degrees $(\mu_i)_i$	$\mathbb{M}_{d-1}$	$\mathbb{MQ}_{\mathbf{ker}}$	$\mathbb{MQ}_{\mathbf{Syl}}$
5 $(2,3)$	74ms	305ms	431ms
10 $(5,5)$	226ms	409ms	1113ms
10 $(1,9)$	187ms	1055ms	614ms
5 $(1,2,2)$	120ms	319ms	663ms
9 $(3,3,3)$	312ms	458ms	1914ms
9 $(1,4,4)$	384ms	987ms	1912ms
9 $(1,1,7)$	304ms	2815ms	1150ms
15 $(5,5,5)$	931ms	1358ms	5989ms
15 $(1,7,7)$	701ms	2311ms	4363ms
15 $(1,1,13)$	946ms	8947ms	2526ms

TABLE 2.2: Comparison of the computation time to build the matrix $\mathbb{M}_{d-1}$ with the computation times of the two algorithms corresponding to build the moving quadric matrices either from kernel computation or by instantiation of Sylvester forms.

In summary, it appears that the new matrix $\mathbb{MQ}_{\mu_n-1}$ is not easier to build compared to the other matrices that are already known, but their computation time remains acceptable. It turns out that these implicit matrix representations are only computed once for a curve and is then stored. So in the end, the computation of the matrix itself is not the most important feature, what is the most important is the efficiency of a matrix when one computes intensively on the curve with it. In the next paragraph, we illustrate this property with the point/curve intersection problem, i.e. by testing whether a given point belongs to the curve. As we will see, for this use the matrices of moving quadrics we introduce behave much better than the previously known matrices.

2.4.2 The drop-of-rank property

What makes the matrices $\mathbb{MQ}_\nu$, $\nu \geqslant \mu_n - 1$, implicit representations is the *drop-of-rank property*: evaluated at a point p, their rank drops, more precisely their rows are linearly dependent, if and only if the point p is on the curve. This property gives a very efficient method to decide whether a point belongs to a curve or not.

In Table 2.3, we compare the computation time for testing if a point belongs to a curve by means of the two moving hyperplanes matrices, $\mathbb{M}_{d-1}$ which is computed without μ-basis and $\mathbb{M}_{\mu_n+\mu_{n-1}-1}$ that requires the computation of a μ-basis, and by means of the smallest matrix of moving hyperplanes and quadrics we obtained, namely $\mathbb{MQ}_{\mu_n-1}$. In all cases we tested, whatever the repartition of the degrees μ_i of the μ-basis, this matrix $\mathbb{MQ}_{\mu_n-1}$ was always more efficient.

Degree d and degrees $(\mu_i)_i$	$\mathbb{M}_{d-1}$	$\mathbb{M}_{\mu_n+\mu_{n-1}-1}$	$\mathbb{MQ}_{\mu_n-1}$
5 (2, 3)	54ms	54ms	22ms
10 (5, 5)	230ms	230ms	62ms
10 (1, 9)	230ms	230ms	121ms
5 (1, 2, 2)	105ms	61ms	22ms
9 (3, 3, 3)	353ms	125ms	59ms
9 (1, 4, 4)	393ms	267ms	78ms
9 (1, 1, 7)	362ms	256ms	171ms
15 (5, 5, 5)	1139ms	377ms	167ms
15 (1, 7, 7)	1127ms	929ms	199ms
15 (1, 1, 13)	1086ms	894ms	534ms

TABLE 2.3: Average time over a hundred random points for testing if a point belongs to the curve.

We notice that deciding whether a point in space belongs to a parameterized curve can be done via a greatest common divisor (GCD) computation once a μ-basis is known. Indeed, let p_1, p_2, p_3 be a μ-basis of a curve parameterization, let q be a point in space and denote by $p_i(q)$ the evaluation of p_i at the point q. Then, the GCD of the three homogeneous polynomials $p_1(q)$, $p_2(q)$ and $p_3(q)$ is a homogeneous polynomial in the variables s, t whose degree is equal to the multiplicity of the point q with respect to the curve, in particular this degree is nonzero if and only if the point q belongs to the curve [82, Theorem 6.4]. However, this method requires exact computations and hence it does not allow to deal with approximate input data. In addition, the use of exact computations makes the computation time strongly dependent on the choice of the point q. To be more concrete, we applied this method to the case of the degree 9 curve with μ-basis of type $(3, 3, 3)$ that is used in Table 2.3. The points are chosen on the curve with five significant digits and are cast to rational numbers for the GCD computation. We observed an average time over a hundred random points of 66s and especially a very high standard deviation of 67s (with a minimum of 15ms and a maximum computation time of 176s). When the matrix $\mathbb{MQ}_2$ is used we observe a standard deviation of 7ms, showing a computation time which is almost independent of the point q. This difference is mostly due to the fact that the matrices of moving hyperplanes and moving quadrics allow to rely on numerical linear algebra tools and are thus capable to deal with approximate data and computations.

Later in Example 2.6.2, we illustrate that given a point $p \in \mathcal{C}$, not only the rank of $\mathbb{MQ}_\nu(p)$, $\nu \geqslant \mu_n - 1$, drops but also its cokernel (left nullspace) allows to recover all the parameters $(s_0 : t_0) \in \mathbb{P}^1$ such that $\Phi(s_0, t_0) = p$, following the approach developed in [18, 16] with the matrices of moving hyperplanes.

2.5 Complexity estimation in terms of height

In order to estimate the complexity for our computations, in what follows a canonical height bound of the terms which appear in the matrix $\mathbb{MQ}_\nu$, is described in terms of maximum height of the f_i's. We recall that matrix $\mathbb{M}_\nu$ of moving hyperplanes at degree ν is computed as the null space of a linear system. Accordingly, we first provide a height bound for an intermediate matrix S_ν, of which null space is $\mathbb{M}_\nu$, and for the null space of a given matrix based on Hermit Normal Form are described. This section assumes the notation of §1.8.

Suppose given an affine curve parameterization over the field of rational numbers

$$\begin{aligned} \varphi : \quad \mathbb{A}^1_{\mathbb{C}_v} &\to \mathbb{A}^m_{\mathbb{C}_v} \\ s &\mapsto \left(\frac{f_1(s)}{f_0(s)}, \ldots, \frac{f_m(s)}{f_0(s)} \right), \end{aligned} \tag{2.13}$$

where the f_i's are the polynomials in s of degree d over $\mathbb{C}_v$.

One can compute $\mathbb{M}_\nu$ as a null space of a linear system. Consider the matrix S_ν as an intermediate coefficient matrix of size $(d+\nu+1)\times(m+1)(\nu+1)$ matrix such that its columns correspond to the polynomials $f_i s^{\nu-j}$ for $1 \leqslant i \leqslant m$ with $0 \leqslant j \leqslant \nu$ and its rows correspond to the monomial basis of degree $d+\nu$, $b := \{s^{d+\nu}, s^{d+\nu-1}, \ldots, 1\}$. Let $h_v(f) := \max_{0\leqslant i\leqslant m}\{0, h_v(f_i)\}$ where v is either prime number p or ∞. Then, by construction of S_ν, it is clear that the height of the matrix S_ν is

$$h_v(S_\nu) = h_v(f).$$

The matrix S_ν is not a square matrix in general, it is square only for $m = 1$, it has number of the columns, denoted by c_ν, greater and equal to the number of the rows, denoted by r_ν. In order to follow the steps of kernel computation we consider Hermit normal form over $\mathbb{Z}$, denoted by HNF (see for instance [27, §2.4.2] or [68, Chapter 2, §6]).

Definition 2.5.1 ([27, Definition 2.4.2.]). *Let k be a field. A polynomial matrix $H \in \mathbb{M}_{m\times n}(k[s])$ with $m \leqslant n$ is in Hermit normal form, if there exist indices $1 \leqslant j_1 \leqslant \cdots \leqslant j_m \leqslant n$ verifying*

- *H is an upper triangular form, i.e. $h_{i,j} = 0$ for $1 \leqslant j < j_i$ and $1 \leqslant i \leqslant r$,*
- *h_{i,j_i} is monic for $1 \leqslant i \leqslant m$,*
- *in each column $\deg(h_{k,j_i}) < \deg(h_{i,j_i})$ for $1 \leqslant k < i \leqslant m$.*

Proposition 2.5.1 ([27, Proposition 2.4.9]). *Let $A \in \mathbb{M}_{m\times n}(\mathbb{Z})$, B be its HNF of form $B = AU$ with $U \in GL_n(\mathbb{Z})$, and r be the first r zero columns of B. Then, a $\mathbb{Z}$-basis for the kernel of A is given by the first r columns of U.*

Let's write the matrix S_ν in form of two submatrices $S_1 \in \mathbb{M}_{r_\nu\times r_\nu}(\mathbb{C}_v)$ and $S_2 \in \mathbb{M}_{r_\nu\times c_\nu - r_\nu}(\mathbb{C}_v)$ such that $S_\nu = (S_1|S_2)$ and S_1 is full rank. Then, the adjoint (adjugate) matrix of S_1, denoted by $\mathrm{adj}(S_1)$, is the transpose of the cofactor matrix of S_1. Consider the matrix U,

$$U := \left[\begin{array}{ccc|ccc} & & & 0 & \cdots & 0 \\ & \mathrm{adj}S_1 & & \vdots & \ddots & \vdots \\ & & & 0 & \cdots & 0 \\ \hline 0 & \cdots & 0 & & & \\ \vdots & \ddots & \vdots & & \mathrm{Id}_{c_\nu - r_\nu} & \\ 0 & \cdots & 0 & & & \end{array}\right],$$

where $\mathrm{Id}_{c_\nu - r_\nu}$ stands for $(c_\nu - r_\nu \times c_\nu - r_\nu)$ identity matrix. Then, we have

$$
\begin{aligned}
S_\nu U &= (S_1|S_2)U \\
&= \left[\begin{array}{ccccc|ccccc}
\det S_1 & 0 & 0 & \cdots & 0 & 0 & \cdots & \cdots & 0 \\
0 & det S_1 & 0 & \cdots & \vdots & \vdots & \ddots & & \vdots \\
\vdots & \ddots & & \ddots & 0 & \vdots & & \ddots & \vdots \\
0 & & \cdots & 0 & \det S_1 & 0 & \cdots & \cdots & 0 \\
\hline
0 & & \cdots & & 0 & & & & \\
\vdots & & \ddots & & \vdots & & K & & \\
0 & & \cdots & & 0 & & & &
\end{array}\right],
\end{aligned}
$$

where last $c_\nu - r_\nu$ columns form a basis for the null space of S_ν by the Proposition 2.5.1.

In order to give a bound for the height the matrix U, we need to give a bound for the height of the matrix $\mathrm{adj}S_1$, which is bounded by the maximum height of $\nu \times \nu$ minors of S_ν. Since a minor of a matrix is just a determinant of one of its submatrices, we start by studying the height of the determinant of any given matrix.

Proposition 2.5.2. *Let $M = (m_{ij})_{1 \leqslant i,j \leqslant n} \in \mathbb{M}_{n\times n}(\mathbb{C}_v)$ be a full rank matrix of which all terms have the height less than given $\mathfrak{h}$. Let v denote either ∞ or prime number p. The height of the determinant of M is bounded by*

$$h_v(\det(M)) \leqslant \max\{0, \log(n!\mathfrak{h}^n).$$

Proof. Recall Leibniz formula

$$\det(M) = \sum_{\sigma \in S_n} (\mathrm{sign}(\sigma_i) \prod_{i=1}^{n} m_{i,\sigma_i}),$$

where S_n is symmetric group of degree n, $m_{i,\sigma_i} \in M$ and sign denotes the sign function of permutation in S_n. Thus, one can compute a bound for the height where $v \in \{\infty, p : \mathrm{p \text{ is prime}}\}$ as follows

$$
\begin{aligned}
h_v(\det(M)) &= h_v(\sum_{\sigma \in S_n} (\mathrm{sign}(\sigma_i) \prod_{i=1}^{n} m_{i,\sigma_i})) \\
&\leqslant \max\{0, \log(\sum_{\sigma \in S_n} |\prod_{i=1}^{n} m_{i\sigma_i}|_v)\} \\
&\leqslant \max\{0, \log(\sum_{\sigma \in S_n} \prod_{i=1}^{n} |m_{i\sigma_i}|_v)\} \\
&\leqslant \max\{0, \log(\sum_{\sigma \in S_n} \mathfrak{h}^n\} \\
&\leqslant \max\{0, \log(n!\mathfrak{h}^n).
\end{aligned}
$$

□

Corollary 2.5.1. *Let $M \in \mathbb{M}_{n\times n}(\mathbb{C}_v)$ be an invertible matrix of which all terms have the height less than given $\mathfrak{h}$. Let v denote either ∞ or prime number p. The height of the adjoint (adjugate) matrix of M, denoted by $\mathrm{adj}(M)$, is bounded by*

$$h_v(\mathrm{adj}(M)) \leqslant \max\{0, \log((n-1)!\mathfrak{h}^{n-1})\}.$$

It remains to find a bound for multiplication of matrices to give a bound for the null space of S_ν based on Hermit normal form as in Proposition 2.5.1.

Proposition 2.5.3. *Let $A = (a_{ij})_{\substack{1\leqslant i\leqslant m\\ 1\leqslant j\leqslant n}} \in \mathbb{M}_{m\times n}(\mathbb{C}_v)$ of height $\mathfrak{h}_{1_v}$ and $B = (b_{ij})_{\substack{1\leqslant i\leqslant n\\ 1\leqslant j\leqslant r}} \in \mathbb{M}_{n\times r}(\mathbb{C}_v)$ of height $\mathfrak{h}_{2_v}$, and let v denote either ∞ or prime number p. Then, the height of $AB \in \mathbb{M}_{m\times r}(\mathbb{C}_v)$ has the following upper bound*

$$h_v(AB) \leqslant \max\{0, \log(n\mathfrak{h}_{1_v}\mathfrak{h}_{2_v})\}.$$

Proof. We have

$$\begin{aligned} h_v(\sum_{i=1}^{n} a_{ij}b_{jk}) &= \max\{0, \log(|\sum_{i=1}^{n} a_{ij}b_{jk}|_v)\} \\ &\leqslant \max\{0, \log(\sum_{i=1}^{n} |a_{ij}b_{jk}|_v)\} \\ &\leqslant \max\{0, \log(\sum_{i=1}^{n} |a_{ij}|_v|b_{jk}|_v)\} \\ &\leqslant \max\{0, \log(n\mathfrak{h}_{1_v}\mathfrak{h}_{2_v})\}. \end{aligned}$$

□

Corollary 2.5.2. *Let v denote either ∞ or prime number p, $\mathfrak{h}_v := h_v(S_\nu)$. The height of the matrix $S_\nu U$, and the height of the null space of S_ν are bounded as follows*

$$h_v(S_\nu U) \leqslant \max\{0, r_\nu\mathfrak{h}_v\log((r_\nu-1)!\mathfrak{h}_v^{r_\nu-1})\}.$$

Proof. It is direct consequence of Proposition 2.5.3 and Corollary 2.5.1. □

The $\ker(S_\nu U)$ corresponding to the parameterization φ in (2.5), consists of $m+1$ blocks of matrices M_i for $0 \leqslant i \leqslant m$ having $\nu+1$ rows. The matrix which corresponds to an implicit representation of the curve defined by the image of φ is of the form

$$\mathbb{M}(\varphi)_\nu(x_1, \ldots, x_m) = M_0 + x_1M_1 + x_2M_2 + \ldots + x_mM_m \tag{2.14}$$

where $\mathbb{C}_v[x_1, \ldots, x_m]$ is the coordinate ring of $\mathbb{A}^m_{\mathbb{C}_v}$.

Proposition 2.5.4. *The height of implicit matrix representation of the curve in $\mathbb{A}^m_{\mathbb{C}_v}$ given by the parameterization φ at degree ν, $\mathbb{M}(\varphi)_\nu$ is bounded by $h_v(\mathbb{M}(\varphi)_\nu) \leqslant h_v(S_\nu U)$ where v is either prime number p or ∞.*

Proof. Since $\mathbb{M}(\varphi)_\nu(x_1, \ldots, x_m)$ is in the form (2.14) and the matrices $\mathbb{M}_i$ for $i = 0, \ldots m$ are coefficient matrices, the entries of $\mathbb{M}_\nu$ are the linear polynomials in x_i's for $i = 1, \ldots, m$. By definition of height of a polynomial, the height $\mathbb{M}(\varphi)_\nu(x_1, \ldots, x_m)$ is bounded by the height of $\max_{0\leqslant i\leqslant n}\{h_v(\mathbb{M}_i)\}$, where v denotes either ∞ or a given prime number p. Hence it is also bounded by the height of $S_\nu U$.

□

In what follows in order to give a bound for the matrix $\mathbb{MQ}_\nu$, we will give a bound for the height of Sylvester forms of μ-basis $p_1, \ldots, p_m$ of the ideal $I := (f_0, \ldots, f_m)$ such that $\deg(p_i) = \mu_i$ for $i = 1, \ldots, m$. We assume that $\mu_1 \leqslant \cdots \leqslant \mu_m$. We recall that $\mathbb{MQ}_\nu$ contains also columns coming from $\mathbb{M}_\nu$. However, since height is non-negative by definition, the height of $\mathbb{MQ}_\nu$ is bounded by the height of Sylvester forms.

Proposition 2.5.5. *The height of* $\mathbb{MQ}_\nu$ *for all* $\mu_m-1 \leqslant \nu \leqslant \mu_m+\mu_{m-1}-1$ *is bounded by the maximum height of sylvester forms of degree* $v_{ij} = \mu_i+\mu_j-\mu_m-1 \leqslant 0$*, denoted by* $h_v(\text{syl})$*, where* v *denotes either* ∞ *or prime number* p*. Then,*

$$h_v(\mathbb{MQ}_\nu) \leqslant \max\{0, \log(2h_v(S_{\mu_m+\mu_{m-1}-1}U))\}.$$

Proof. The proof is immediate using Proposition 2.5.3 and the structure of sylvester forms defined in §2.2.2, more precisely determinant of two-by-two matrices obtained via corresponding μ-basis. In order to find an upper bound for μ-basis we used an upper bound for $\mathbb{M}_{\mu_m+\mu_{m-1}-1}$ using $h_v(S_{\mu_m+\mu_{m-1}-1}U)$ (see Proposition 2.1.6). Also, $h_v(\mathbb{MQ}_\nu)) \leqslant h_v(\mathbb{MQ}_{\mu_m+\mu_{m-1}-1})$ for all $\mu_m - 1 \leqslant \nu \leqslant \mu_m + \mu_{m-1} - 1$, since $\mathbb{MQ}_{\mu_m+\mu_{m-1}-1}$ is the biggest possible. □

2.5.1 Experiments on height computation

I considered random 15×15 matrices of coefficients over $\mathbb{Z}$ having standard absolute value of around 360 digits. The experiments over 100 examples showed that the bounds for the standard height of the determinant in Proposition 2.5.2, for the standard height of the multiplication of two such matrices in Proposition 2.5.3 and for the standard height of the multiplication of a matrix with its adjoint in Corollary 2.5.2 are sharp. More precisely, the ratio of the standard height bound for determinant formula by the standard height of the determinant by computation is 1.06211687282368 over 100 examples. Similarly, the ratio of the standard height bound for the multiplication of two such matrices by the standard height of the multiplication matrix is 1.00258054192892 over 100 examples.

With the similar matrices, the ratio of the standard height bound for the multiplication of a matrix with its adjoint by the standard height of their multiplication is 1.02168229040873 over 100 examples. For the reason of the computation time, I did not consider the matrices of size more then 15×15.

Lastly, in order to validate Corollary 2.5.2, I considered 100 random curve parameterizations of degree 6 in three-dimensional space given by random polynomials having standard absolute value of around 360 digits. Then, the ratio of the standard height bound for $S_\nu U$ in Corollay 2.5.2 by standard height of S_ν is 1.10820622054175 over 100 examples. We can see that it is slightly more than for general matrices (which is 1.02168229040873 for a matrix having the same number of columns as S_ν under consideration.) as we have previously explained. It is because S_ν consists of 4 blocks of Sylvester matrix. Moreover, in this section we used Hermit normal form in order to give a bound for the null space of a given matrix, which is eventually bigger than what the height of the null space of S_ν via SageMath command of kernel, for which the ratio is 9.03771875205243 over 100 examples.

2.6 Applications

We emphasize that all the applications that are discussed in [16] with the matrices of moving hyperplanes also apply with our extended family of matrices $\mathbb{MQ}$ built with moving hyperplanes and moving quadrics. For instance, the curve/curve intersection problem and the computation of the self-intersection locus of a parameterized curve, computation of multiplicity of singular points on a parameterized curve can be solved with these new matrices following essentially the same algorithms; we refer the reader to [16] for more details. We also give an equivalent distance notion for distance from a point to a parameterized curve in terms of $\mathbb{MQ}$.

2.6.1 Curve/curve intersection

Let's consider two rational algebraic curves given by parameterizations Φ_1 and Φ_2 defined by polynomials of degree d_1 and d_2 respectively. Let's assume that a μ-basis of the ideal generated by the coordinates of Φ_1 is of degrees (μ_1, μ_2, μ_3) with $\mu_1 \leqslant \mu_2 \leqslant \mu_3$. In order to compute the intersection of $\mathcal{C}_1$ and $\mathcal{C}_2$, we substitute the parameterization Φ_2 into $\mathbb{MQ}_{\mu_3-1}(\Phi_1)$. Let's denote this substitution matrix as $\mathbb{MQ}_{\mu_3-1}(\Phi_1;\Phi_2)$. Since $\mathbb{MQ}_{\mu_3-1}(\Phi_1)$ has entries both linear and quadratic, the entries of $\mathbb{MQ}_{\mu_3-1}(\Phi_1;\Phi_2)$ are of degree at most $2\times d_2$. Moreover, by Proposition 2.2.1 and equation (2.7), the matrix $\mathbb{MQ}_{\mu_3-1}(\Phi_1)$ has $\max(0,\mu_1+\mu_2-\mu_3)+\mu_1+\mu_2$ quadratic columns and $2\mu_3-\mu_1-\mu_2$ linear columns, hence in total $\max(0,\mu_1+\mu_2-\mu_3)+2\mu_3$ columns (see Definition 2.2.2). In addition, for a degree d general curve in three dimensional space, i.e. $\mu_i \approx \frac{d}{3}$ for $i=1,2,3$, the corresponding $\mathbb{MQ}_{\mu_3-1}$ has almost d columns.

Let us recall companion matrices of a given $r\times c$ polynomial matrix M whose entries are at most degree d in $k[s,t]$. We can write a polynomial in $k[s,t]$ with matrix coefficients of size $r\times c$, such that

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

where M_i is a matrix of coefficients in k of the same size as M for all $i=0,\ldots,d$. Let I_d denotes the $d\times d$ identity matrix. Then, we the following matrices are called companion matrices of M

$$\begin{bmatrix} 0 & I_d & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & I_d \\ M_0^T & M_1^T & \cdots & M_{d-1}^T \end{bmatrix}, \begin{bmatrix} I_d & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & I_d & 0 \\ 0 & \cdots & 0 & -M_d^T \end{bmatrix}.$$

Then the companion matrices of $\mathbb{MQ}_{\mu_3-1}(\Phi_1;\Phi_2)$ are of size $\mu_3\times\max(0,\mu_1+\mu_2-\mu_3)+2\mu_3$.

One may consider two companion matrices of $\mathbb{MQ}_{\mu_3-1}(\Phi_1;\Phi_2)$ which are not square matrices (see for instance [16]). We use Kronecker form in order to reduce the companion matrices into the smallest full rank square matrices (see [63]). We call these reduced forms as *regular part of the companion matrices*. Also, we recall that $\mathbb{MQ}_{\mu_3-1}$ has always less or equal number of columns than $\mathbb{M}_{\mu_3+\mu_2-1}$ (see for instance 2.1). Then, the companion matrices of the smallest matrix representations $\mathbb{MQ}_{\mu_3-1}$ and $\mathbb{M}_{\mu_3+\mu_2-1}$ have $d_2\cdot\mu_3$ and $d_2(\mu_2+\mu_3)$ rows respectively. The bigger the difference between μ_2 and μ_3 we have, the smallest pencil of companion matrices we need to consider by using $\mathbb{MQ}_{\mu_3-1}$ which is almost the half size of the pencil of companion matrices obtained via $\mathbb{M}_{\mu_3+\mu_2-1}$. Then generalized eigenvalues computation of pencil of reduced companion matrices allow us to compute the parameter value of the intersection of $\mathcal{C}_1$ and $\mathcal{C}_2$. We call the procedure of computing the parameter values from a matrix representation the *inversion process*. Here, we discussed in a three dimensional space, however it is also true for higher dimensions.

Example 2.6.1. *Let us consider the rational curve $\mathcal{C}_1$ given in Example 2.3.1 and denote its parameterization as Φ_1, and the twisted cubic which is parameterized by the rational map*

$$\Phi_2(s,t) \mapsto (s^3 : s^2t : st^2 : t^3),$$

where μ-basis of ideal $I = (s^3, s^2t, st^2, t^3)$ are in degrees $\mu_1 = \mu_2 = \mu_3 = 2$. We compute $\mathbb{MQ}_\nu(\Phi_1)$ for $\nu = \mu_3 - 1 = 2 - 1 = 1$.

$$\mathbb{MQ}_1(\Phi_1) = \left(\begin{array}{ccc} x_0x_1 - \frac{1}{10}x_1^2 + \frac{9}{10}x_2^2 + \frac{3}{5}x_0x_3 - \frac{9}{2}x_1x_3 - \frac{9}{4}x_2x_3 & & \\ -\frac{3}{10}x_1^2 + \frac{27}{10}x_2^2 - \frac{9}{10}x_0x_3 - \frac{3}{2}x_1x_3 - \frac{9}{5}x_2x_3 & & \end{array} \right.$$

$$\begin{array}{ccc} \frac{1}{10}x_1^2 - \frac{9}{10}x_2^2 + \frac{9}{10}x_0x_3 + \frac{6}{5}x_1x_3 & x_0x_2 - \frac{1}{2}x_1x_3 & \\ x_0x_1 - \frac{1}{5}x_1^2 + \frac{9}{5}x_2^2 - \frac{21}{10}x_0x_3 - \frac{9}{4}x_1x_3 - \frac{9}{20}x_2x_3 & -\frac{1}{2}x_0x_3 - \frac{1}{2}x_1x_3 & \end{array}$$

$$\left. \begin{array}{ccc} \frac{1}{2}x_0x_3 & x_1x_2 + 3x_2^2 - 3x_2x_3 - 3x_2x_3 & -\frac{1}{2}x_1x_3 - \frac{3}{2}x_2x_3 \\ x_0x_2 - \frac{3}{2}x_0x_3 - \frac{1}{2}x_1x_3 & \frac{3}{2}x_1x_3 - \frac{3}{2}x_2x_3 & x_1x_2 + 3x_2^2 - \frac{5}{2}x_1x_3 - \frac{3}{2}x_2x_3 \end{array} \right).$$

is a 2×6 matrix of rank having both linear and quadratic entries in x, y, z, w. This example is taken from [16, Example 24]. In order to compute the intersection of $\mathcal{C}_1$ and $\mathcal{C}_2$, we substitute the parameterization Φ_2 into $\mathbb{MQ}_1(\Phi_1)$, i.e. we substitute $x = s^3, y = s^2t, z = st^2, w = t^3$ into $\mathbb{MQ}_1(\Phi_1)$. Then, the substitution matrix $\mathbb{MQ}_1(\Phi_1; \Phi_2)$ has entries of degree $2 \times 3 = 6$, where 2 is coming from the fact that $\mathbb{MQ}_1(\Phi)$ has quadratic entries, and 3 is the degree of the polynomials defining the parameterization Φ_2. The companion matrices of $\mathbb{MQ}_1(\Phi_1; \Phi_2)$ are of size 6×36. One may also consider the substitution matrix obtained only by the moving hyperplanes following Φ_1 for $\nu = 3$, denote it as $\mathbb{M}_3(\Phi_1)$. In this case according to [16, Example 24] the companion matrices of $\mathbb{M}_3(\Phi_1; \Phi_2)$ of size 12×18, before Kronecker reduction.

2.6.2 Multiplicity of singular points and inversion

Let $\mathcal{C}$ be a rational algebraic curve in $\mathbb{P}^3_k$ given by the parameterization Φ. Let μ_i be the degrees of a μ-basis of ideal generated by the coordinates of Φ. With the previous notation, for a point $p \in \mathbb{P}^3_k$, one may use $\mathbb{MQ}_\nu$ such that $\nu \geqslant \mu_3 - 1$ in order to compute the multiplicity of p on $\mathcal{C}$. This computation is quicker than dealing with the matrix of hyperplanes $\mathbb{M}_{\mu_3+\mu_2-1}$, see Table 2.1.

Theorem 2.6.1 ([16, Theorem 13])**.** *Given a point $p \in \mathbb{P}^3_k$. Let's denote the multiplicity of p on $\mathcal{C}$ by $m_p(\mathcal{C})$. Then for all integer $\nu \geqslant \mu_n - 1$, we have*

$$\operatorname{rank}(\mathbb{MQ}_\nu(p)) = \nu + 1 - m_p(\mathcal{C}),$$

or equivalently the drop-of-rank at p is equal to $m_p(\mathcal{C})$.

Let us take $\nu = \mu_n - 1$. If $\operatorname{rank}(\mathbb{MQ}_\nu(p)) = \mu_n - 1$, then the curve $\mathcal{C}$ passes once through the point p whose pre-image can be computed by using the suitable proportion in the basis in which $\mathbb{MQ}_\nu$ is constructed. For instance, if we consider $\mathbb{MQ}_\nu$ in monomial basis $\{s^\nu, s^{\nu-1}t, \ldots, t^\nu\}$, then the proportion of first two terms of $\operatorname{coker}(\mathbb{MQ}_\nu)$ gives us $\frac{s}{t}$ coordinate of p. If $\operatorname{rank}(\mathbb{MQ}_\nu(p)) \leqslant \mu_n - 2$, then the curve $\mathcal{C}$ passes more than once through the point p and we need to do generalized eigenvalues computation by considering again similar proportions as in the case where $\mathcal{C}$ passes through the point p only once. We refer the reader for instance to [18, §3.3] for further details about inversion.

Example 2.6.2. *Consider the lemniscate-like space curve $\mathcal{C}$ given by*

$$\begin{aligned} F_0(s,t) &= (t^2+s^2)(t^4+s^2),\\ F_1(s,t) &= t(t^2-s^2)^2,\\ F_2(s,t) &= t(t^4-s^4),\\ F_3(s,t) &= 3s^4+t^4. \end{aligned}$$

This curve has a self-intersection point at $p := (1:0:0:1)$. The matrix of moving quadrics $\mathbb{MQ}_2$ is of size 3×6 and, when evaluated at p, has a cokernel given by

$$v_1 = (v_{1,1}, v_{1,2}, v_{1,3}) = (1,0,1)$$

and

$$v_2 = (v_{2,1}, v_{2,2}, v_{2,3}) = (0,1,0).$$

None of these vectors are of the form $v = (s^2, st, t^2)$ but they are linear combinations of the two vectors corresponding to the evaluation of the form v at the two pre-images parameters of p. Therefore, to retrieve these two pre-images one can solve the eigenvalue problem

$$\operatorname{rank}(t\Delta_0 - s\Delta_1) < 2$$

where

$$\Delta_0 = \begin{pmatrix} v_{1,1} & v_{1,2} \\ v_{2,1} & v_{2,2} \end{pmatrix}, \quad \Delta_1 = \begin{pmatrix} v_{1,2} & v_{1,3} \\ v_{2,2} & v_{2,3} \end{pmatrix}.$$

We deduce that the pre-images of p correspond to the parameters $(s_0 : t_0) = (1:1)$ and $(s_1 : t_1) = (1:-1)$.

Finally, we notice that the matrix $\mathbb{MQ}_1$ is of size 2×6 and satisfies to the drop-of-rank property. Its rank drops by 2 after evaluation at p, thus it is equal to the null matrix when evaluated at p. Therefore, in this case the matrix is too small to allow the inversion of a multiple point and hence it is necessary to increase the degree ν by one. In general a matrix $\mathbb{MQ}_\nu$ allows to invert points having at most ν pre-images.

The curve $\mathcal{C}$ has a self-intersection at the point $p := (1,0,0,1)$. The matrix $\mathbb{MQ}_1(\Phi)$ is of size 1×6 The rank of $\mathbb{MQ}_1(\Phi)(1:0:0:1)$ drops 2. Hence, $\mathcal{C}$ passes twice through p, i.e. $m_p(\mathcal{C}) = 2$.

2.6.3 Singular factors

Given an algebraic rational curve in $\mathbb{P}^n_k$ with a parameterization Φ. We compute the matrix representation $\mathbb{MQ}_{\mu_n-1}(\Phi)$. Then substitute the parameterization of Φ into $\mathbb{MQ}_{\mu_n-1}(\Phi)$. Let's denote this substitution matrix as $\mathbb{MQ}^\Phi$. Then for all points on $\mathcal{C}$, $\mathbb{MQ}^\Phi$ verifies the drop-of-rank property. According to the results in [18, §5.2], we can write the singular factors of the parameterization Φ, using the Smith form of $\mathbb{MQ}^\Phi(s,1)$ and $\mathbb{MQ}^\Phi(1,t)$ as follows.

Example 2.6.3 ([18, Example 23])**.** *Let consider the curve $\mathcal{C}$ given with the parameterization*

$$\Phi(s:t) \mapsto (s^5 : s^3t^2 : s^2t^3 : t^5).$$

The μ-basis of $I = (s^5, s^3t^2, s^2t^3, t^5)$ has $\mu_1 = 1, \mu_2 = 2, \mu_3 = 2$. Then,

$$\mathbb{MQ}_1(\Phi) = \begin{bmatrix} -x_2^2 & -x_1^2 & -x_1x_2 + x_0x_3 & -x_2^2 & x_1x_3 \\ x_1 & x_0x_2 & 0 & x_0x_3 & -x_2^2 \end{bmatrix}.$$

Then we substitute the parameterization Φ *into* $\mathbb{MQ}_1(\Phi)$*, and we obtain*

$$\begin{bmatrix} -s^2t^3 & -s^6t^4 & 0 & -s^4t^6 & s^3t^7 \\ s^3t^2 & s^7t^3 & 0 & s^5t^5 & -s^4t^6 \end{bmatrix}$$

The Smith form of $\mathbb{MQ}_1(\Phi)(s:1)$ *and* $\mathbb{MQ}_1(\Phi)(1:t)$ *are respectively*

$$\begin{bmatrix} s^2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} t^2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

Then the singular factors of $\mathcal{C}$ *is given by* s^2t^2 *and* $\mathcal{C}$ *has two singular points* $(0:0:0:1)$ *and* $(1:0:0:0)$ *of multiplicity 2. Since we have almost half size implicit matrix than in [18, Example 23], we need to deal with half size Smith forms.*

2.6.4 Distance function

We have mentioned that the implicitization of parameterized space curves is much more delicate since a space curve is not given by a single equation in $\mathbb{C}$. However we can give a single implicit equation defining the curve over field of real numbers (see [18, §11]). For this reason, we will define the *real evaluation function of* $\mathbb{MQ}_\nu$ and in the sequel we will follow the notation of [18]. Consider a space curve $\mathcal{C}$ given by a parameterization Φ.

Definition 2.6.1 ([18, Definition 2])**.** *To any point* $p \in \mathbb{R}^3$*, we associate the real evaluation function of* $\mathbb{MQ}_\nu$*,* $\nu \in \mathbb{N}$

$$\begin{array}{rccl} \delta_{\mathbb{MQ}_\nu}: & \mathbb{R}^3 & \to & \mathbb{R}_{\geqslant 0} \\ & p & \mapsto & \delta_{\mathbb{MQ}_\nu}(p) := \prod_{i=1}^{\nu+1} \sigma_i(\mathbb{MQ}_\nu(p)), \end{array}$$

where $\sigma_i(\mathbb{MQ}_\nu(p))$*'s are the singular values of* $\mathbb{MQ}_\nu(p)$*.*

Since, the singular values are non-negative and the rank of a matrix is the positive integer i giving the maximum nonzero singular value of the given matrix, we have

$$\delta_{\mathbb{MQ}_\nu}(p) = 0 \Longleftrightarrow p \in \mathcal{I}m(\Phi).$$

Thus, the real evaluation function behaves like a distance function between the point p and the curve $\mathcal{C}$. Now we will define the square of the real evaluation function which yields a real implicit equation defining $\mathcal{I}m(\Phi)$ (see [18, §4.3]). Consider,

$$\delta_{\mathbb{MQ}_\nu}(p)^2 = \prod_{i=1}^{\nu+1} \sigma_i(\mathbb{MQ}_\nu(p))^2 = \det(\mathbb{MQ}_\nu(p)\mathbb{MQ}_\nu(p)^T).$$

Here, we remark that $\mathbb{MQ}_\nu(p)\mathbb{MQ}_\nu(p)^T$ is a real valued square matrix.

Theorem 2.6.2 ([18, Theorem 1])**.** *The real algebraic set*

$$\{(x,y,z) \in \mathbb{R}^3 : \delta_{\mathbb{MQ}_\nu}(x,y,z) = 0\} \in \mathbb{R}^3$$

is a degree $2(\nu+1)$ *real implicit equation of the curve* $\mathcal{C}$*.*

With respect to the smallest matrix representations $\mathbb{MQ}_{\mu_3-1}$ and $\mathbb{M}_{\mu_3+\mu_2-1}$, we can write degree $2 \cdot \mu_3$ and respectively degree $\mu_2 + \mu_3$ real implicit equations. For a general space curve, these two equations are almost the same degree. However, as

much as the difference between μ_2 and μ_3 increases then the degree of $\delta_{\mathbb{MQ}_{\mu_3-1}}$ is much bigger then the degree of $\delta_{\mathbb{M}_{\mu_3+\mu_2-1}}$.

By [18, Theorem 2 in §4.4], more precisely using Łojasiewicz inequality we can show that the square of real evaluation function behaves similar to a distance function. Hence, it defines an equivalent distance to Euclidean distance.

In the sequel of this thesis mainly the distance problem is studied. More precisely, in the next chapter, a new algebraic method to compute the Euclidean distance between a point and a rational algebraic surface in three dimensional space is introduced. For that purpose, similar implicit matrices built from some certain syzygies will be used.

CHAPTER 3

Rational maps in three dimensional space

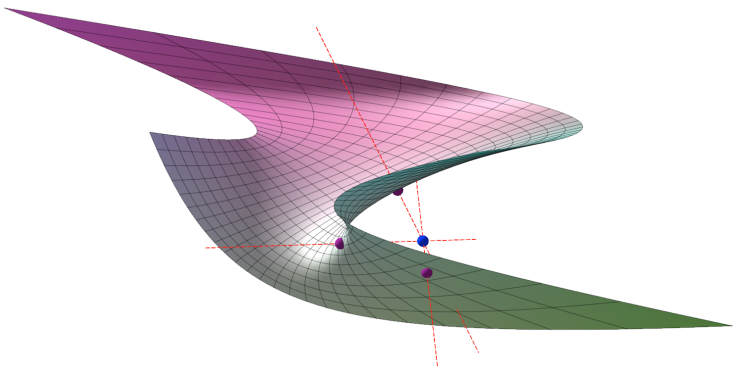


FIGURE 1. Orthogonal projections of a point onto a bi-quadratic rational tensor-product Bézier surface patch.

Algebraic methods to orthogonally project points onto rational algebraic surfaces already appeared in the literature [38, 62], including by means of congruence of normal lines [78, 76], but they are facing computational efficiency problems very quickly as the defining degree of surface parameterizations is increasing, because of the intrinsic complexity of the problem. A good measure of this complexity is provided by the Euclidean distance degree introduced in [38] (see also [54]); for instance, in general a point has 94 orthogonal projections onto a rational bi-cubic surface (a surface in $\mathbb{P}^3$ parameterized over $\mathbb{P}^1 \times \mathbb{P}^1$ by bi-homogeneous polynomials of bi-degree $(3,3)$). In order to push these limits, this chapter introduces a preprocessing step in which an elimination matrix dedicated to a given rational surface, and depending linearly in the space coordinates, is generated. The effective computation of the orthogonal projections of a point p on this surface is then highly accelerated in comparison to other methods without preprocessing step ([78]), since it consists in the instantiation of this elimination matrix at p and the use of fast and robust numerical linear algebra methods, such as singular value decompositions, eigenvalue and eigenvector numerical calculations.

The methodology we develop in this chapter is based on matrix representations of rational maps and their fibers. These representations have already been studied in various settings, see e.g. [3, 75, 2, 5, 16, 4, 13, 12, 73]. Roughly, they correspond to a presentation matrix of certain graded slices of the symmetric algebra of the ideal I generated by the defining equations of the map under consideration. The determination of the appropriate graded slices is the main difficulty in this approach and it requires a thorough analysis of the syzygy modules of I. In this chapter, guided by

our application to orthogonal projection onto rational surfaces, we consider trivariate maps whose source space is equal to $\mathbb{P}^2 \times \mathbb{P}^1$, a bi-graded algebraic structure, or $\mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$, a tri-graded algebraic structure. In addition we also need to consider maps that have a one-dimensional base locus, because general congruences of normal lines to rational surfaces have positive dimensional base loci. This latter requirement is definitely the more challenging one. To the best of our knowledge, only [23] studied rational maps with one-dimensional base locus, and all the previous published related works considered multi-graded rational maps with a base locus of dimension at most zero, i.e. the base locus consists in finitely many points or is empty. The main results are Theorem 3.2.1 and Theorem 3.2.2. They provide the expected matrix representations under some assumptions on the curve component of the base locus, namely either being globally generated by three linear combinations of the four defining equations of I up to saturation, or either being a complete intersection. Coming back to our application, these theorems provide the theoretical foundations of a new methodology for computing orthogonal projections onto a rational algebraic surface.

This chapter is organized as follows. In Section 3.1 we introduce congruences of normal lines to a rational surface, provide corresponding Macaulay2 code, give some examples and explain why it is useful for computing orthogonal projections of points. Then, in Section 3.2 the matrix representations of these congruences of normal lines are defined and the main results are stated. Their proof requires a fine analysis of the vanishing of certain local cohomology modules which is presented in Section 3.3. In Section 3.4 we give some technical results on global sections of curves in a product of projective spaces in order to shed light on some assumptions that appear in Theorem 3.2.1 and Theorem 3.2.2. Finally, Section 3.5 is devoted to the description of an algorithm for computing the orthogonal projections of a point onto a rational surface which is parameterized by either $\mathbb{P}^2$ (triangular surface) or $\mathbb{P}^1 \times \mathbb{P}^1$ (tensor-product surface).

Lastly, this worked has been accepted for publication in SIAM Journal on Applied Algebra and Geometry, and preprint can be found at `https://arxiv.org/abs/1903.08107v2`.

3.1 Congruence of normal lines to a rational surface

In this section, we introduce congruences of normal lines to a rational surface $\mathcal{S}$, i.e. parameterizations of the 2-dimensional family of normal lines to $\mathcal{S}$. Given a point p in space, it allows us to translate the computation of the orthogonal projections of p onto $\mathcal{S}$ as the computation of the pre-images of p via these congruences. In order to use algebraic methods, in particular elimination techniques, we first describe the homogenization of these congruence maps, as well as their base loci, for two classes of rational surfaces that are widely used in CAGD: triangular and tensor-product rational surfaces.

3.1.1 Congruences of normal lines

We assume that we are given the following affine parameterization of a rational surface $\mathcal{S}$ in the three dimensional space

$$\begin{array}{rccc} \phi: & \mathbb{R}^2 & \dashrightarrow & \mathbb{R}^3 \\ & (u,v) & \mapsto & \left(\dfrac{f_1(u,v)}{f_0(u,v)}, \dfrac{f_2(u,v)}{f_0(u,v)}, \dfrac{f_3(u,v)}{f_0(u,v)}\right), \end{array} \tag{3.1}$$

where f_0, f_1, f_2, f_3 are polynomials in the variables u, v. At each nonsingular point p on $\mathcal{S}$ one can define a normal line which is the line through p spanned by a normal vector $\nabla(p)$ to the tangent plane to $\mathcal{S}$ at p. The congruence of normal lines to $\mathcal{S}$ is then the rational map

$$\begin{array}{rccc} \psi: & \mathbb{R}^3 & \dashrightarrow & \mathbb{R}^3 \\ & (u,v,t) & \mapsto & \phi(u,v) + t\nabla(\phi(u,v)). \end{array} \tag{3.2}$$

If the parameterization ϕ is given, then there are many ways to formulate explicitly the above parameterization, depending on the choice of the expression of $\nabla(\phi(u,v))$. The more commonly used one is the cross product of the two vectors $\frac{\partial\phi}{\partial u}$ and $\frac{\partial\phi}{\partial v}$ that are linearly independent at almost all points in the image of ϕ. Thus, we get

$$\psi(u,v,t) = \phi(u,v) + t \cdot \frac{\partial\phi}{\partial u} \wedge \frac{\partial\phi}{\partial v}(u,v).$$

Nevertheless, with the following example we emphasize that depending on ϕ, a more specific and simple (for instance in terms of degree) expression of ψ may be used.

Example 3.1.1. *The unit sphere can be parameterized by*

$$\phi(u,v) = \left(\frac{2u}{1+u^2+v^2}, \frac{2v}{1+u^2+v^2}, \frac{-1+u^2+v^2}{1+u^2+v^2}\right).$$

Since $\phi(u,v)$ is also a normal vector to the unit sphere at the point $\phi(u,v)$, a simpler expression than (3.2) for the congruence of normal lines is

$$\psi(u,v,t) = t\phi(u,v).$$

The main interest of the congruence of normal lines is that it allows to translate the computation of orthogonal projection onto the surface $\mathcal{S}$ as an inversion problem. More precisely, given a point $p \in \mathbb{R}^3$, its orthogonal projection on $\mathcal{S}$ can be obtained from its pre-images via ψ. Indeed, if $\phi(u_0, v_0)$ is an orthogonal projection of p on $\mathcal{S}$ for some parameters $(u_0, v_0) \in \mathbb{R}^2$, then that means that p belongs to the normal line to $\mathcal{S}$ at the point $\phi(u_0, v_0)$. Therefore, there exists t_0 such that the point $(u_0, v_0, t_0) \in \mathbb{R}^3$ is a pre-image of p via ψ.

In general, the computation of the orthogonal projections of a point onto a rational surface is a difficult and computationally expensive task. A measure of its complexity is given by the expected number of orthogonal projections of a general point p. This number is called the *Euclidean distance degree* of the surface; it has been introduced and carefully studied in [38] (see also [54]). In Table 3.1 the Euclidean distance degree of surfaces we consider in this chapter are recalled.

3.1.2 Homogenization to projective spaces

The geometric approach we propose for computing orthogonal projections of points onto a rational surface via the "fibers" of the corresponding congruence of normal lines relies on algebraic methods that require to work in an homogeneous setting. Thus, it is necessary to homogenize the parameterizations ϕ and ψ defined by (3.1) and (3.2) respectively.

Regarding the homogenization of the map ϕ, the canonical choice is to homogenize its source to the projective plane $\mathbb{P}^2$, but there are other possible choices depending on the support of the polynomial f_i. We focus on the two main classes of rational

surfaces that are used in Computer-Aided Geometric Design (CAGD). The first class is called the class of *rational triangular surfaces*. It corresponds to polynomials of the form

$$f_k(u,v) = \sum_{\substack{0\leqslant i,j\leqslant d \\ 0\leqslant i+j\leqslant d}} c_{k,i,j} u^i v^j, \quad k = 0,\dots,3$$

where d is a given positive integer, the degree of the polynomials $f_k(u,v)$. The canonical homogenization of the map ϕ is then of the form

$$\begin{array}{rcl} \Phi : \mathbb{P}^2 & \dashrightarrow & \mathbb{P}^3 \\ (w:u:v) & \mapsto & (F_0:F_1:F_2:F_3) \end{array}$$

where the F_i's are homogeneous polynomials in $\mathbb{R}[u,v,w]$ of degree d. If $F_0 = w^d$, equivalently if $f_0(u,v) = 1$ in (3.1), then one speaks of *non-rational triangular surfaces*. This terminology refers to the fact that in this case the parameterization ϕ is defined by polynomials and not by rational functions as in the general case.

The second class of rational surfaces is called the class of *rational tensor-product surfaces*. It corresponds to polynomials of the form

$$f_k(u,v) = \sum_{0\leqslant i\leqslant d_1,\ 0\leqslant i\leqslant d_2} c_{k,i,j} u^i v^j, \quad k = 0,\dots,3$$

where (d_1,d_2) is a couple of positive integers, the bi-degree of the polynomials $f_k(u,v)$. In this case, the canonical homogenization of the map ϕ is of the form

$$\begin{array}{rcl} \Phi : \mathbb{P}^1 \times \mathbb{P}^1 & \dashrightarrow & \mathbb{P}^3 \\ (\overline{u}:u) \times (\overline{v}:v) & \mapsto & (F_0:F_1:F_2:F_3) \end{array}$$

where the F_i's are here bi-homogeneous polynomials in $\mathbb{R}[\overline{u},u;\overline{v},v]$ of bi-degree (d_1,d_2). If $F_0 = \overline{u}^{d_1}\overline{v}^{d_2}$, equivalently if $f_0(u,v) = 1$ in (3.1), then one speaks of *non-rational tensor-product surfaces*.

From now on we set the following notation. The map Φ is a rational map from the projective variety X to $\mathbb{P}^3$, where X stands either for either $\mathbb{P}^2$ or $\mathbb{P}^1 \times \mathbb{P}^1$. Thus, when we use the notion of degree over X, it has to be understood with respect to these two possibilities, i.e. either the single grading of $\mathbb{P}^2$ or the bi-grading of $\mathbb{P}^1 \times \mathbb{P}^1$. The homogeneous polynomials F_0, F_1, F_2, F_3 defining the map Φ are homogeneous polynomials in the coordinate ring of X of degree $\mathbf{d}$, this latter being either a positive integer or a couple of positive integers, depending on X.

For the sake of completeness, we recall from [38] the Euclidean distance degree of Φ In Table 3.1. As we already mentioned, it is closely related to our problem.

	Triangular surface	Tensor-product surface
Non-Rational	$(2d-1)^2$	$8d_1d_2 - 2(d_1+d_2) + 1$
Rational	$7d^2 - 9d + 3$	$14d_1d_2 - 6(d_1+d_2) + 4$

TABLE 3.1: Euclidean distance degree of non-rational and rational triangular surfaces of degree $d \geqslant 1$ and tensor-product surfaces $(d_1,d_2) \geqslant (1,1)$, respectively.

Once the choice of homogenization of Φ from X to $\mathbb{P}^3$ is done, it is natural to homogenize ψ as a rational map from $X \times \mathbb{P}^1$ to $\mathbb{P}^3$, which means geometrically that the congruence of normal lines to the surface is seen as a family of projective lines parameterized by X. This map is hence of the form

$$\begin{array}{rcl} \Psi : X \times \mathbb{P}^1 & \dashrightarrow & \mathbb{P}^3 \\ \xi \times (\bar{t} : t) & \mapsto & (\Psi_0 : \Psi_1 : \Psi_2 : \Psi_3) \end{array} \tag{3.3}$$

where the polynomials Ψ_i's are bi-graded: they are graded with respect to X and to $\mathbb{P}^1$. Observe that these polynomials are actually linear forms with respect to $\mathbb{P}^1$.

3.1.3 Explicit homogeneous parameterizations

To describe the rational map Ψ more explicitly, we need to consider projective tangent planes to the surface $\mathcal{S}$ and projective lines that are orthogonal to them.

Let $\xi \in X$ and $p = \Phi(\xi)$ be a smooth point on $\mathcal{S} \subset \mathbb{P}^3$. An equation of the projective tangent space to $\mathcal{S}$ at p, denoted $\mathrm{T}_p\mathcal{S}$, can be obtained from the Jacobian matrix of the polynomials F_0, F_1, F_2, F_3 (see [46, Chapter 14]). If $X = \mathbb{P}^2$, i.e. for rational triangular surfaces, then this equation is given by

$$\begin{vmatrix} \partial_u F_0 & \partial_u F_1 & \partial_u F_2 & \partial_u F_3 \\ \partial_v F_0 & \partial_v F_1 & \partial_v F_2 & \partial_v F_3 \\ \partial_w F_0 & \partial_w F_1 & \partial_w F_2 & \partial_w F_3 \\ x_0 & x_1 & x_2 & x_3 \end{vmatrix} = x_0\Delta_0(\xi) + x_1\Delta_1(\xi) + x_2\Delta_2(\xi) + x_3\Delta_3(\xi) = 0.$$

Observe that the signed minors $\Delta_i(u, v, w)$ are homogeneous polynomials of degree $D := 3(d-1)$, as the F_i's are supposed to be of degree d.Similarly, If $X = \mathbb{P}^1 \times \mathbb{P}^1$, i.e. for rational tensor-product surfaces, then an equation of $\mathrm{T}_p\mathcal{S}$ is given by the vanishing of the determinant

$$\begin{vmatrix} \partial_u F_0 & \partial_u F_1 & \partial_u F_2 & \partial_u F_3 \\ \partial_{\overline{u}} F_0 & \partial_{\overline{u}} F_1 & \partial_{\overline{u}} F_2 & \partial_{\overline{u}} F_3 \\ \partial_v F_0 & \partial_v F_1 & \partial_v F_2 & \partial_v F_3 \\ x_0 & x_1 & x_2 & x_3 \end{vmatrix} = 0.$$

Compared to the previous case, there is here a redundancy because two Euler equalities hold, one with respect to $(u, \overline{u})$ and the other with respect to $(v, \overline{v})$. Actually, this redundancy implies that the above determinant vanishes if $\overline{v} = 0$. Therefore, an equation of $\mathrm{T}_p\mathcal{S}$ is given by the formula

$$\begin{vmatrix} \partial_u F_0 & \partial_u F_1 & \partial_u F_2 & \partial_u F_3 \\ \partial_{\overline{u}} F_0 & \partial_{\overline{u}} F_1 & \partial_{\overline{u}} F_2 & \partial_{\overline{u}} F_3 \\ \partial_v F_0 & \partial_v F_1 & \partial_v F_2 & \partial_v F_3 \\ x_0 & x_1 & x_2 & x_3 \end{vmatrix} = \overline{v}(x_0\Delta_0(\xi) + x_1\Delta_1(\xi) + x_2\Delta_2(\xi) + x_3\Delta_3(\xi)) = 0$$

where the signed (and reduced) minors $\Delta_i(\overline{u}, u; \overline{v}, v)$ are bi-homogeneous polynomials of bi-degree $D := (3d_1 - 2, 3d_2 - 2)$.

Example 3.1.2. *The following* Macaulay2 *code computes the signed minors of the Jacobian matrix of the homogeneous polynomials F_0, F_1, F_2, F_3 of bidegree (d_1, d_2) in $\mathbb{P}^1 \times \mathbb{P}^1$ over the field of rational numbers.*

```
S=QQ[u,uu,v,vv,Degrees=>{{1,0},{1,0},{0,1},{0,1}}]
f=random(S^{{d1,d2}},S^{{0,0},{0,0},{0,0},{0,0}});\\

JMfull=jacobian f;
JM=JMfull^{0,1,2};
df0 = determinant(JM_{1,2,3}) // vv;
df1 = (-1)*determinant(JM_{0,2,3}) // vv;
df2 = determinant(JM_{0,1,3}) // vv;
df3 = (-1)*determinant(JM_{0,1,2}) // vv;
J = ideal (df0,df1,df2,df3);
```

Now, to characterize normal lines to $\mathcal{S}$ we use the following property.

Lemma 3.1.1. *Let H be a hyperplane in $\mathbb{P}^3$ of equation $a_0x_0+a_1x_1+a_2x_2+a_3x_3 = 0$ and L be a line in $\mathbb{P}^3$ that are not contained in the hyperplane at infinity $V(x_0) \subset \mathbb{P}^3$. Then, L is orthogonal to H, in the sense that their restrictions to the affine space $\mathbb{P}^3 \setminus V(x_0)$ are orthogonal, if and only if the projective point $(0 : a_1 : a_2 : a_3)$ belongs to L.*

Proof. Let H_1, H_2 be two hyperplanes of equations $\sum_{i=0}^{3} \alpha_i x_i = 0$ and $\sum_{i=0}^{3} \beta_i x_i = 0$ respectively, and suppose that their intersection is exactly the line L. After restriction to the affine space $\mathbb{P}^3 \setminus V(x_0)$, we have that the direction of L is given by the cross product of the two vectors $(\alpha_1, \alpha_2, \alpha_3)$ and $(\beta_1, \beta_2, \beta_3)$. Therefore, we deduce that L is orthogonal to H if and only if the vector (a_1, a_2, a_3) is orthogonal to both vectors $(\alpha_1, \alpha_2, \alpha_3)$ and $(\beta_1, \beta_2, \beta_3)$, which precisely means that the projective point $(0 : a_1 : a_2 : a_3)$ belongs to the hyperplanes H_1 and H_2, hence to L. □

From the above property, we deduce that there are two points that belong to $\mathcal{S}$, namely the point $\Phi(\underline{x}) = (F_0(\xi) : F_1(\underline{x}) : F_2(\underline{x}) : F_3(\underline{x}))$ and the point $(0 : \Delta_1(\underline{x}) : \Delta_2(\underline{x}) : \Delta_3(\underline{x}))$. Therefore, we can derive explicit rational parameterizations of the congruence of normal lines (3.3) as follows.

If $X = \mathbb{P}^2$ and $d \geqslant 2$, we get the following parameterization for the congruence of normal lines of a triangular rational surface

$$\begin{array}{rcl} \Psi : \mathbb{P}^2 \times \mathbb{P}^1 & \dashrightarrow & \mathbb{P}^3 \\ (w : u : v) \times (\bar{t} : t) & \mapsto & (\Psi_0 : \Psi_1 : \Psi_2 : \Psi_3) \end{array} \tag{3.4}$$

where

$$\Psi_0 = \bar{t}w^{2d-3}F_0(u, v, w),\ \Psi_i = \bar{t}w^{2d-3}F_i(u, v, w) + t\Delta_i(u, v, w),\ i = 1, 2, 3$$

are bi-homogeneous polynomials of bi-degree $(3d - 3, 1)$ over $\mathbb{P}^2 \times \mathbb{P}^1$.

If $X = \mathbb{P}^1 \times \mathbb{P}^1$ and $d_1 \geqslant 1$ and $d_2 \geqslant 1$ we get the following parameterization for the congruence of normal lines of a tensor-product rational surface

$$\begin{array}{rcl} \Psi : \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1 & \dashrightarrow & \mathbb{P}^3 \\ (\overline{u} : u) \times (\overline{v} : v) \times (\bar{t} : t) & \mapsto & (\Psi_0 : \Psi_1 : \Psi_2 : \Psi_3) \end{array} \tag{3.5}$$

where

$$\begin{aligned} \Psi_0 &= \bar{t}\overline{u}^{2d_1-2}\overline{v}^{2d_2-2}F_0(\overline{u}, u; \overline{v}, v), \\ \Psi_i &= \bar{t}\overline{u}^{2d_1-2}\overline{v}^{2d_2-2}F_i(\overline{u}, u; \overline{v}, v) + t\Delta_i(\overline{u}, u; \overline{v}, v),\ i = 1, 2, 3 \end{aligned}$$

are tri-homogeneous polynomials of degree $(3d_1 - 2, 3d_2 - 2, 1)$ over $\mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$.

Example 3.1.3. *The following* MACAULAY2 *code computes the homogeneous parameterization of the congruence of normal lines to the given rational tensor-product surface of bidegree (d_1, d_2) over $\mathbb{Q}$, where J denotes the Jacobian matrix of the homogeneous polynomials F_0, F_1, F_2, F_3.*

```
S=QQ[u,uu,v,vv,t,tt,Degrees=>{{1,0,0},{1,0,0},{0,1,0},{0,1,0},
{0,0,1},{0,0,1}}]
Psi0=tt*uu^(2*d1-2)*vv^(2*d2-2)*F_(0,0);
for i from 1 to 3 list tt*uu^(2*d1-2)*vv^(2*d2-2)*F_(0,i)+t*J_i;
```

We emphasize that the above parameterizations hold for general triangular and tensor-product rational surfaces, so that some simplifications may appear in some particular cases. For instance, such simplifications are obtained with the so-called *non-rational* triangular and tensor-product surfaces. These surfaces are characterized by the fact that their affine parameterizations in space can be given by polynomials after de-homogenization. Equivalently, this means that the homogeneous polynomial F_0 is independent of the variables u and v. Thus, if $X = \mathbb{P}^2$ then $F_0 = w^d$ and if $X = \mathbb{P}^1 \times \mathbb{P}^1$ then $F_0 = \overline{u}^{d_1}\overline{v}^{d_2}$. Under this assumption, the polynomials Δ_1, Δ_2 and Δ_3 have a common factor, namely w^{d-1} if $X = \mathbb{P}^2$, and $\overline{u}^{d_1-1}\overline{v}^{d_2-1}$ if $X = \mathbb{P}^1 \times \mathbb{P}^1$. Therefore, this common factor propagates to the polynomials $\Psi_0, \ldots, \Psi_3$ and hence the corresponding parameterization Ψ of the congruence of normal lines is given by polynomials of bi-degree $(2d-2, 1)$ if $X = \mathbb{P}^2$ and of tri-degree $(2d_1 - 1, 2d_2 - 1, 1)$ if $X = \mathbb{P}^1 \times \mathbb{P}^1$. We summarize all these considerations in Table 3.2.

$\deg(\Psi_i)$	Triangular surface	Tensor-product surface
Non-rational	$(2d-2, 1)$	$(2d_1 - 1, 2d_2 - 1, 1)$
Rational	$(3d-3, 1)$	$(3d_1 - 2, 3d_2 - 2, 1)$

TABLE 3.2: Degree of the parameterizations of the congruence Ψ of normal lines associated to non-rational/rational triangular/tensor-product surfaces.

3.1.4 Base locus

Consider the map Ψ defined by (3.3). Its base locus $\mathcal{B}$ is the subscheme of $X \times \mathbb{P}^1$ defined by the polynomials $\Psi_0, \Psi_1, \Psi_2, \Psi_3$. As we will see in the next section, this locus is of particular importance in our syzygy-based approach for studying the "fibers" of Ψ.

Without loss of generality, $\mathcal{B}$ can be assumed to be of dimension at most one by simply removing the common factor of the polynomials $\Psi_0, \ldots, \Psi_3$, if any. It is clear from (3.4) and (3.5) that $\mathcal{B}$ is always one-dimensional. In the following lemma we describe the curve component of $\mathcal{B}$ when the corresponding surface parameterization Φ is sufficiently general. Below, inequalities between tuples of integers are understood component-wisely.

Lemma 3.1.2. *For a general rational surface parameterization Φ, the curve component of the base locus $\mathcal{B}$ of its corresponding congruence of normal lines Ψ as defined in (3.4) and (3.5), is given by*

- *the ideal* (w^{2d-3}, t) *if* $X = \mathbb{P}^2$ *and* $d \geqslant 2$,
- *the ideal* $(\overline{u}^{2d_1-2}\overline{v}^{2d_2-2}, t)$ *if* $X = \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$ *and* $(d_1, d_2) \geqslant (1, 1)$.

Similarly, for a general non-rational surface parameterization Φ*, the base locus* $\mathcal{B}$ *of* Ψ *is a one-dimensional subscheme of* $X \times \mathbb{P}^1$ *whose curve component is defined by*

- *the ideal* (w^{d-2}, t) *if* $X = \mathbb{P}^2$ *and* $d \geqslant 2$,
- *the ideal* $(\overline{u}^{d_1-1}\overline{v}^{d_2-1}, t)$ *if* $X = \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$ *and* $(d_1, d_2) \geqslant (1, 1)$.

Proof. We only consider the case $X = \mathbb{P}^2$ and Φ rational, the other cases are similar. By (3.4), we have the matrix equality

$$\begin{pmatrix} \Psi_0 & \Psi_1 & \Psi_2 & \Psi_3 \end{pmatrix} = \begin{pmatrix} \bar{t}w^{2d-3} & t \end{pmatrix} \cdot \begin{pmatrix} F_0 & F_1 & F_2 & F_3 \\ 0 & \Delta_1 & \Delta_2 & \Delta_3 \end{pmatrix}$$

so that the ideal $(\Psi_0, \ldots, \Psi_3) : (\bar{t}w^{2d-3}, t)$ is contained in the ideal generated by $\Psi_0, \ldots, \Psi_3$ and the 2-minors of the matrix

$$\mathbb{F} := \begin{pmatrix} F_0 & F_1 & F_2 & F_3 \\ 0 & \Delta_1 & \Delta_2 & \Delta_3 \end{pmatrix}.$$

Then, the first row of $\mathbb{F}$ vanishes at base points of the surface paramaterization Φ, which are assumed to be finitely many. The second row of $\mathbb{F}$ vanishes at the singular points of the image of Φ and at the points where the tangent plane is of equation $x_0 = 0$; if Φ is sufficiently general then these latter points are also finitely many. Finally, the two rows of $\mathbb{F}$ are proportional at finitely many points such that $F_0 = 0$, always assuming that Φ is sufficiently general. Therefore, we deduce that the curve component of the ideal defined by the Ψ_i's is defined by the ideal (w^{2d-3}, t) in $\mathbb{P}^2 \times \mathbb{P}^1$. □

Remark 3.1.1. *If* $X = \mathbb{P}^1 \times \mathbb{P}^1$ *and* $(d_1, d_2) = (1, 1)$ *then there is no curve component in the base locus* $\mathcal{B}$ *for both non-rational and rational surface parameterizations. The same holds if* $X = \mathbb{P}^2$ *and* $d = 2$ *for non-rational surface parameterizations.*

3.2 Fibers and matrices of syzygies

In this section, we extend our framework and suppose that we are given an homogeneous parameterization

$$\begin{array}{rcl} \Psi : X \times \mathbb{P}^1 & \dashrightarrow & \mathbb{P}^3 \\ \xi \times (\bar{t} : t) & \mapsto & (\Psi_0 : \Psi_1 : \Psi_2 : \Psi_3)\,, \end{array} \tag{3.6}$$

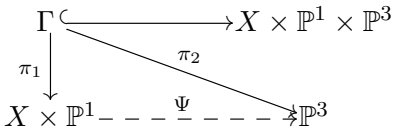
where X stands for $\mathbb{P}^2$ or $\mathbb{P}^1 \times \mathbb{P}^1$ and the Ψ_i's are homogeneous polynomials in the coordinate ring of $X \times \mathbb{P}^1$ for all $i = 0, 1, 2, 3$. The coordinate ring R_X of X is equal to $k[u, v, w]$ or $k[\overline{u}, u; \overline{v}, v]$, respectively, depending on X where k is a field. The coordinate ring of $\mathbb{P}^1$ is denoted by $R_1 = k[\overline{t}, t]$ and hence the coordinate ring of $X \times \mathbb{P}^1$ is the polynomial ring $R := R_X \otimes_k R_1$. Thus, the polynomials $\Psi_0, \Psi_1, \Psi_2, \Psi_3$ are multi-homogeneous polynomials of degree $(\boldsymbol{\delta}, e)$, where $\boldsymbol{\delta}$ refers to the degree with respect to X, which can be either an integer if $X = \mathbb{P}^2$, or either a couple of integers if $X = \mathbb{P}^1 \times \mathbb{P}^1$.

In what follows, we assume that Ψ is a dominant map. We denote by I the ideal generated by $\Psi_0, \Psi_1, \Psi_2, \Psi_3$ in R. The base locus $\mathcal{B}$ of the map Ψ is the subscheme

of $X \times \mathbb{P}^1$ defined by I. Without loss of generality, we assume that $\mathcal{B}$ is of dimension at most one. Our aim is to provide a matrix-based representation of the finite fibers of Ψ, by means of the syzygies of the ideal I.

3.2.1 Fiber of a point

The map Ψ being a rational map, its fibers are not well defined. To give a proper definition of the fiber of a point under Ψ, we need to consider the graph of Ψ that we denote by $\Gamma \subset X \times \mathbb{P}^1 \times \mathbb{P}^3$. The defining equations of this graph are known to be the equations of the multi-graded Rees algebra of the ideal I of R, denoted $\mathrm{Rees}(I)$. It has two canonical projections π_1 and π_2 onto $X \times \mathbb{P}^1$ and $\mathbb{P}^3$ respectively:



Thus, the fiber of a point $p \in \mathbb{P}^3$ is defined through the regular map π_2. More precisely, if $\kappa(p)$ denotes the residue field of p, *the fiber of* $p \in \mathbb{P}^3$ is the subscheme

$$\mathfrak{F}_p \quad := \mathrm{Proj}(\mathrm{Rees}(I) \otimes \kappa(p)) \subset X \times \mathbb{P}^1. \tag{3.7}$$

From a computational point of view, the equations of the Rees algebra $\mathrm{Rees}(I)$ are very difficult to get. Therefore, it is useful to approximate the Rees algebra $\mathrm{Rees}(I)$ by the corresponding symmetric algebra of the ideal I (see §1.2.), that we denote by $\mathrm{Sym}(I)$. This approximation amounts to keep among the equations of the Rees algebra only those that can be generated, as an ideal, by those that are *linear* with respect to the third factor $\mathbb{P}^3$. Thus, as a variation of the standard definition (3.7) of the fiber of a point $p \in \mathbb{P}^3$, we consider the subscheme

$$\mathfrak{L}_p \quad := \mathrm{Proj}(\mathrm{Sym}(I) \otimes \kappa(p)) \subset X \times \mathbb{P}^1 \tag{3.8}$$

that we call *the linear fiber of* p. We emphasize that the fiber $\mathfrak{F}_p$ is always contained in the linear fiber $\mathfrak{L}_p$ of a point p, and that they coincide if the ideal I is locally a complete intersection at p.

3.2.2 Matrices built from syzygies

Given a point p in $\mathbb{P}^3$, the dimension and the degree of its linear fiber $\mathfrak{L}_p$ can be read from its Hilbert polynomial. The evaluation of this polynomial, and more generally of its corresponding Hilbert function, can be done by computing the rank of a collection of matrices that we introduce. They are built from the syzygies of the ideal I. An additional motivation to consider these matrices is that they also allow to compute effectively the points defined by the linear fiber $\mathfrak{L}_p$, hence the pre-images of p via Ψ, if $\mathfrak{L}_p$ is finite. This property will be detailed in Section 3.5.

Let $k[x_0, x_1, x_2, x_3]$ be the coordinate ring of $\mathbb{P}^3$. The symmetric algebra $\mathrm{Sym}(I)$ of the ideal $I = (\Psi_0, \ldots, \Psi_3)$ of R is the quotient of the polynomial ring $R[x_0, x_1, x_2, x_3]$ by the ideal generated by the linear forms in the x_i's whose coefficients are syzygies of the polynomials $\Psi_0, \ldots, \Psi_3$ of degree $(\mathbf{d}, e)$. More precisely, consider the graded map

$$R(-\boldsymbol{\delta}, -e)^4 \quad \to \quad R$$

$$(g_0, g_1, g_2, g_3) \quad \mapsto \quad \sum_{i=0}^{3} g_i \Psi_i \tag{3.9}$$

and denote its kernel by Z_1, which is nothing but the first module of syzygies of I. Setting $\mathcal{Z}_1 := Z_1(\boldsymbol{\delta}, e) \otimes R[x_0, \ldots, x_3]$ and $\mathcal{Z}_0 = R[x_0, \ldots, x_3]$, then the symmetric algebra $\mathrm{Sym}(I)$ admits the following multi-graded presentation

$$\begin{array}{rcl} \mathcal{Z}_1(-1) & \xrightarrow{\varphi} & \mathcal{Z}_0 \to \mathrm{Sym}(I) \to 0 \\ (g_0, g_1, g_2, g_3) & \mapsto & \displaystyle\sum_{i=0}^{3} g_i x_i. \end{array} \tag{3.10}$$

where the shift in the grading of $\mathcal{Z}_1$ is with respect to the grading of $k[x_0, \ldots, x_3]$.

Definition 3.2.1. *The graded part of the map φ in any degree $(\boldsymbol{\mu}, \nu)$ with respect to $R = R_X \otimes R_1$ gives a map of free $k[x_0, \ldots, x_3]$-modules. Its matrix, which depends on a choice of basis, is denoted by $\mathbb{M}_{(\boldsymbol{\mu},\nu)}(\Psi)$, or simply by $\mathbb{M}_{(\boldsymbol{\mu},\nu)}$. Its entries are linear forms in $k[x_0, \ldots, x_3]$.*

As a consequence of (3.10), for any point $p \in \mathbb{P}^3$ the corank of the matrix $\mathbb{M}_{(\boldsymbol{\mu},\nu)}$ evaluated at p, that we denote by $\mathbb{M}_{(\boldsymbol{\mu},\nu)}(p)$, is equal to the Hilbert function of the linear fiber $\mathfrak{L}_p$ in degree $(\boldsymbol{\mu}, \nu)$. Because the Hilbert function is equal to its corresponding Hilbert polynomial for suitable degrees $(\boldsymbol{\mu}, \nu)$ (see [9, Theorem 4.1.3]), the corank of the matrix $\mathbb{M}_{(\boldsymbol{\mu},\nu)}(p)$ is expected to stabilize to a constant value if $\mathfrak{L}_p$ is finite. In what follows, we provide effective bounds for this stability property under suitable assumptions.

Consider $\mathbb{M}_{(\boldsymbol{\mu},0)}(\Psi)$ where $\boldsymbol{\mu}$ is a degree over X and Ψ is a parameterization of congruence of normal lines to a given parametric surface of degree $\boldsymbol{\delta}$ as in (3.3), hence $\boldsymbol{\delta}$ is a degree over X. Lastly, as previously described in §2.5, $\mathbb{M}_{(\boldsymbol{\mu},0)}(\Psi)$, can be also computed via the null space of the intermediary coefficient matrix $S_{(\boldsymbol{\mu},1)}$ as follows.

- If $X = \mathbb{P}^2$, then $S_{(\boldsymbol{\mu},1)}$ is a $(\boldsymbol{\mu}+\boldsymbol{\delta}+1)(\boldsymbol{\mu}+\boldsymbol{\delta}+2) \times 2(\boldsymbol{\mu}+1)(\boldsymbol{\mu}+2)$ matrix such that its columns correspond to the polynomials $F_i u^{\boldsymbol{\mu}-i} v^k w^{i-k}$ with $0 \leqslant k \leqslant i \leqslant \boldsymbol{\mu}$, and its rows correspond to the homogeneous monomial basis of degree $\boldsymbol{\delta} + \boldsymbol{\mu}$, $b := \{w^{\boldsymbol{\delta}+\boldsymbol{\mu}}, uw^{\boldsymbol{\delta}+\boldsymbol{\mu}-1}, u^2 w^{\boldsymbol{\delta}+\boldsymbol{\mu}-2}, \ldots, u^{\boldsymbol{\delta}+\boldsymbol{\mu}}, vw^{\boldsymbol{\delta}+\boldsymbol{\mu}-1}, vuw^{\boldsymbol{\delta}+\boldsymbol{\mu}-2}, vu^2 w^{\boldsymbol{\delta}+\boldsymbol{\mu}-3}, \ldots, vu^{\boldsymbol{\delta}+\boldsymbol{\mu}-1}, \ldots, v^{\boldsymbol{\delta}+\boldsymbol{\mu}}\}$.
- If $X = \mathbb{P}^1 \times \mathbb{P}^1$, then $\boldsymbol{\mu} = (\mu_1, \mu_2)$, $\boldsymbol{\delta} = (\delta_1, \delta_2)$ and $S_{(\boldsymbol{\mu},1)}$ is a $2(\mu_1+\delta_1+1)(\mu_2+\delta_2+1) \times 4(\mu_1+1)(\mu_2+1)$ matrix such that its columns correspond to the polynomials $F_i u^{\mu_1-i} \bar{u}^i v^{\mu_2-j} \bar{v}^j$ with $0 \leqslant i \leqslant \mu_1$ and $0 \leqslant j \leqslant \mu_2$ and its rows correspond to the homogeneous tensor-product monomial basis of degree $\boldsymbol{\delta}+\boldsymbol{\mu}$ (component wisely addition), $b := \{\bar{u}^{\delta_1+\mu_1} \bar{v}^{\delta_2+\mu_2}, u\bar{u}^{\delta_1+\mu_1-1} \bar{v}^{\delta_2+\mu_2}, u^2 \bar{u}^{\delta_1+\mu_1-2} \bar{v}^{\delta_2+\mu_2}, \ldots, \bar{u}^{\delta_1+\mu_1} v\bar{v}^{\delta_2+\mu_2-1}, u\bar{u}^{\delta_1+\mu_1-1} v\bar{v}^{\delta_2+\mu_2-1}, \ldots, u^{\delta_1+\mu_1} v^{\delta_2+\mu_2}\}$.

We will denote $\mathbb{M}_{(\boldsymbol{\mu},0)}(\Psi)$ as $\mathbb{M}$ for the simplicity. By construction, the null space of $S_{(\boldsymbol{\mu},1)}$ consists of four blocks of matrix $\mathbb{M}_0, \mathbb{M}_1, \mathbb{M}_2, \mathbb{M}_3$ along its rows in basis b such that

- if $X = \mathbb{P}^2$, then $b := \{w^{\boldsymbol{\mu}}, uw^{\boldsymbol{\mu}-1}, u^2 w^{\boldsymbol{\mu}-2}, \ldots, u^{\boldsymbol{\mu}}, vw^{\boldsymbol{\mu}-1}, vuw^{\boldsymbol{\mu}-2}, vu^2 w^{\boldsymbol{\mu}-3}, \ldots, vu^{\boldsymbol{\mu}-1}, \ldots, v^{\boldsymbol{\mu}}\}$, and
- if $X = \mathbb{P}^1 \times \mathbb{P}^1$, then $b := \{\bar{u}^{\mu_1} \bar{v}^{\mu_2}, u\bar{u}^{\mu_1-1} \bar{v}^{\mu_2}, u^2 \bar{u}^{\mu_1-2} \bar{v}^{\mu_2}, \ldots, \bar{u}^{\mu_1} v\bar{v}^{\mu_2-1}, u\bar{u}^{\mu_1-1} v\bar{v}^{\mu_2-1}, \ldots, u^{\mu_1} v^{\mu_2}\}$.

Then,

$$\mathbb{M} = \mathbb{M}_0 x_0 + \mathbb{M}_1 x_1 + \mathbb{M}_2 x_2 + \mathbb{M}_3 x_3.$$

Example 3.2.1. *We give* MACAULAY2 *code to compute the matrix* $\mathbb{M}_{(\boldsymbol{\mu},0)}$ *of a parameterization of the congruence of normal lines to a given rational tensor-product surface* Ψ *and at given degree* $(\boldsymbol{\mu}, 0)$ *(see Corrollary 3.5.1 for this degree choice). For the parameterization* Ψ *see Example 3.1.3, the bidegree* $(D1, D2)$ *see Table 3.2, and lastly for bidegree* $\boldsymbol{\mu} = (\mu_1, \mu_2)$ *see Table 3.3.*

```
S=QQ[u,uu,v,vv,t,tt,Degrees=>{{1,0,0},{1,0,0},{0,1,0},{0,1,0},{0,0,1},
{0,0,1}}]
P=matrix{{Psi0,Psi1,Psi2,Psi3}}
D1=3*d1-2, D2=3*d2-2
B=basis({mu1,mu2,0},S)
SM=B*P_(0,0)|B*P_(0,1)|B*P_(0,2)|B*P_(0,3)
(smu,Smu)=coefficients(SM,Variables=>{u_S,uu_S,v_S,vv_S,t_S,tt_S},
Monomials=>basis({mu1+D1,mu2+D2,1},S))
Smu
rank Smu
MM=syz Smu
```

Example 3.2.2. *Let's consider the parameterization of Segre variety as non-rational* $(1,1)$ *tensor-product surface* $\mathcal{S}$*, i.e.*

$$\begin{array}{rcl} \Phi := \mathbb{P}^1 \times \mathbb{P}^1 & \to & \mathbb{P}^3 \\ (\bar{u} : u) \times (\bar{v} : v) & \mapsto & (\bar{u}\bar{v} : u\bar{v} : v\bar{u} : uv). \end{array} \tag{3.11}$$

Then, at non singular point ξ*, the determinant of the Jacobian matrix of the coordinates of* Φ *gives*

$$\begin{vmatrix} 0 & \bar{v} & 0 & v \\ \bar{v} & 0 & v & 0 \\ 0 & 0 & \bar{u} & u \\ x_0 & x_1 & x_2 & x_3 \end{vmatrix} = \bar{v}(x_0\Delta_0(\xi) + x_1\Delta_1(\xi) + x_2\Delta_2(\xi) + x_3\Delta_3(\xi)),$$

where $\Delta_0 = -uv$*,* $\Delta_1 = \bar{u}v$*,* $\Delta_2 = u\bar{v}$ *and* $\Delta_3 = -\bar{u}\bar{v}$*. Hence, the parameterization* Ψ *of the congruence of normal lines is*

$$\begin{array}{rcl} \Phi := \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1 & \to & \mathbb{P}^3 \\ (\bar{u} : u) \times (\bar{v} : v) \times (\bar{t}, t) & \mapsto & (\bar{t}\bar{u}\bar{v} : \bar{t}u\bar{v} + t\bar{u}v : \bar{t}v\bar{u} + t\bar{u}\bar{v} : \bar{t}uv - t\bar{u}\bar{v}) \end{array} \tag{3.12}$$

of degree $(1,1,1)$ *on* $\mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$*. Then the corresponding matrix representation* $\mathbb{M}_{(2,2,0)}$ *of the finite fiber of* Ψ *at point* $p = (p_0 : p_1 : p_2 : p_3)$ *in* $\mathbb{P}^3$ *is*

$$\mathbb{M}_{(2,2,0)} := \begin{bmatrix} 0 & -p_0 & 0 & 0 & 0 \\ 0 & 0 & -p_0 & p_1 & 0 \\ p_0 & -p_0 & 0 & -p_3 & 0 \\ 0 & 0 & 0 & -p_2 & -p_0 \\ 0 & p_3 & 0 & 0 & 0 \\ -p_1 & p_1 & p_3 & -p_2 & -p_0 \\ -p_0 & 0 & 0 & p_3 & 0 \\ p_2 & 0 & -p_0 & p_1 & p_3 \\ 0 & 0 & p_2 & 0 & p_1 \end{bmatrix}.$$

3.2.3 Main results

We recall that I is the ideal of $R = R_X \otimes R_1$ generated by the defining polynomials of the map Ψ, i.e. $I := (\Psi_0, \Psi_1, \Psi_2, \Psi_3)$. The irrelevant ideal of $X \times \mathbb{P}^1$ is denoted by B; it is equal to the product of ideals $(u, v, w) \cdot (\bar{t}, t)$ if $X = \mathbb{P}^2$, or to the product $(\overline{u}, u) \cdot (\overline{v}, v) \cdot (\bar{t}, t)$ if $X = \mathbb{P}^1 \times \mathbb{P}^1$. The notation I^{sat} stands for the saturation of the ideal I with respect to the ideal B, i.e. $I^{\text{sat}} = (I : B^\infty)$. The homogeneous polynomials $\Psi_0, \Psi_1, \Psi_2, \Psi_3$ are of degree $(\boldsymbol{\delta}, e)$, where $\boldsymbol{\delta}$ denotes the degree with respect to X and e denotes the degree with respect to $\mathbb{P}^1$. We recall that inequalities between tuples of integers are understood component-wisely.

The base locus of Ψ is the subscheme of $X \times \mathbb{P}^1$ defined by the ideal I; it is denoted by $\mathcal{B}$. Without loss of generality, $\mathcal{B}$ is assumed to be of dimension at most one; if $\dim(\mathcal{B}) = 1$ then we denote by $\mathcal{C}$ its top unmixed one-dimensional curve component.

Definition 3.2.2. *The curve $\mathcal{C} \subset X \times \mathbb{P}^1$ is said to have* no section in degree $< (\boldsymbol{a}, b)$ *if $H^0(\mathcal{C}, \mathcal{O}_{\mathcal{C}}(\boldsymbol{\alpha}, \beta)) = 0$ for any degree $(\boldsymbol{\alpha}, \beta)$ such that $\boldsymbol{\alpha} < \boldsymbol{a}$ and $\beta < b$, i.e. if $\mathcal{C}$ has no global section in degree $< (\boldsymbol{a}, b)$.*

For the sake of simplicity in what follows we introduce the following notation.

Notation 3.2.1. *Let r be a positive integer. For any $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_r) \in (\mathbb{Z} \cup \{-\infty\})^r$ we set*

$$\mathbb{E}(\boldsymbol{\alpha}) := \{\boldsymbol{\zeta} \in \mathbb{Z}^r \mid \zeta_i \geqslant \alpha_i \text{ for all } i = 1, \ldots, r\}.$$

It follows that for any $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ in $(\mathbb{Z} \cup \{-\infty\})^r$ we have that $\mathbb{E}(\boldsymbol{\alpha}) \cap \mathbb{E}(\boldsymbol{\beta}) = \mathbb{E}(\boldsymbol{\gamma})$ where $\gamma_i = \max\{\alpha_i, \beta_i\}$ for all $i = 1, \ldots, r$, i.e. $\boldsymbol{\gamma}$ is the maximum of $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ component-wisely.

We are now ready to state our main results.

Theorem 3.2.1. *Assume that we are in one of the two following cases:*

(a) The base locus $\mathcal{B}$ is finite, possibly empty,

(b) $\dim(\mathcal{B}) = 1$, $\mathcal{C}$ has no section in degree $< (\mathbf{0}, e)$ and $I^{sat} = I'^{sat}$ where I' is an ideal generated by three general linear combinations of the polynomials $\Psi_0, \ldots, \Psi_3$.

Let p be a point in $\mathbb{P}^3$ such that $\mathfrak{L}_p$ is finite, then

$$\operatorname{corank} \mathbb{M}_{(\boldsymbol{\mu}, \nu)}(p) = \deg(\mathfrak{L}_p)$$

for any degree $(\boldsymbol{\mu}, \nu)$ such that

- *if $X = \mathbb{P}^2$,*

$$(\mu, \nu) \quad \in \mathbb{E}(3\delta - 2, e - 1) \cup \mathbb{E}(2\delta - 2, 3e - 1). \tag{3.13}$$

- *if $X = \mathbb{P}^1 \times \mathbb{P}^1$,*

$$\begin{aligned}(\boldsymbol{\mu}, \nu) \quad \in \mathbb{E}(3\delta_1 - 1, 2\delta_2 - 1, e - 1) \cup \mathbb{E}(2\delta_1 - 1, 3\delta_2 - 1, e - 1) \\ \cup \mathbb{E}(2\delta_1 - 1, 2\delta_2 - 1, 3e - 1).\end{aligned} \tag{3.14}$$

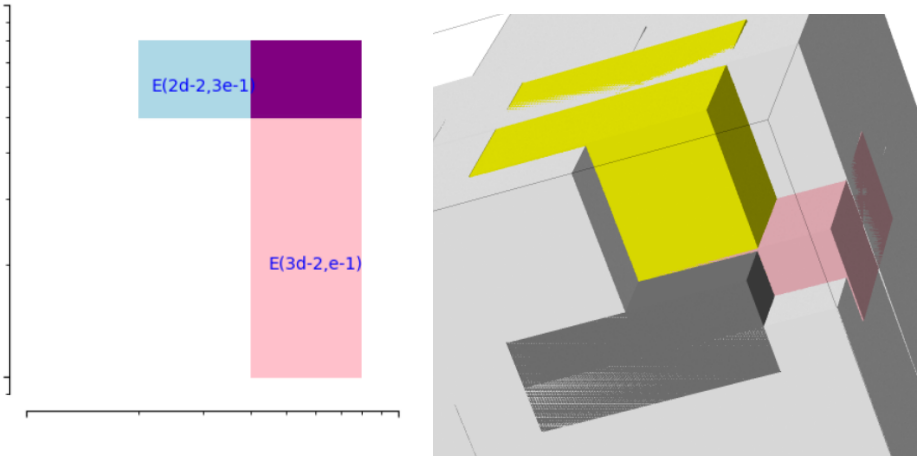


FIGURE 3.2: $(\boldsymbol{\mu}, \nu)$ degrees with respect to $X = \mathbb{P}^2$ and $X = \mathbb{P}^1 \times \mathbb{P}^1$ respectively are given. For $X = \mathbb{P}^2$, blue, pink and purple area correspond to $\mathbb{E}(2\delta - 2, 3e - 1)$, $\mathbb{E}(3\delta - 2, e - 1)$ and $\mathbb{E}(2\delta - 2, 3e - 1) \cap \mathbb{E}(3\delta - 2, e - 1)$ respectively. For $X = \mathbb{P}^1 \times \mathbb{P}^1$, (μ, ν) degrees are chosen in the complementary of the colored volumes, i.e. the union (3.14).

Proof. By (3.10), the corank of the matrix $\mathbb{M}_{(\boldsymbol{\mu},\nu)}(p)$ is equal to the Hilbert function of $\mathrm{Sym}(I) \otimes \kappa(p)$ at $(\boldsymbol{\mu}, \nu)$, that we denote by $HF_{\mathrm{Sym}(I)\otimes\kappa(p)}(\boldsymbol{\mu}, \nu)$. Moreover, since $\mathfrak{L}_p$ is assumed to be finite, the Hilbert polynomial of $\mathrm{Sym}(I) \otimes \kappa(p)$, denoted $HP_{\mathrm{Sym}(I)\otimes\kappa(p)}(\boldsymbol{\mu}, \nu)$, is a constant polynomial which is equal to the degree of $\mathfrak{L}_p$. Now, the Grothendieck-Serre formula shows that for any degree $(\boldsymbol{\mu}, \nu)$ we have the equality (see for instance [6, Proposition 4.26])

$$HP_{\mathrm{Sym}(I)\otimes\kappa(p)}(\boldsymbol{\mu}, \nu) = HF_{\mathrm{Sym}(I)\otimes\kappa(p)}(\boldsymbol{\mu}, \nu) - \sum_{i \geqslant 0} (-1)^i HF_{H^i_B(\mathrm{Sym}(I)\otimes\kappa(p))}(\boldsymbol{\mu}, \nu).$$

Therefore, the theorem will be proved if we show that the Hilbert functions of the local cohomology modules $H^i_B(\mathrm{Sym}(I) \otimes \kappa(p))$ vanish for all integers i and all degrees $(\boldsymbol{\mu}, \nu)$ satisfying to the conditions stated in the theorem. This property is the content of Theorem 3.3.1 whose proof is postponed to Section 3.3. □

In the case where the base locus $\mathcal{B}$ has dimension one, the assumption $I^{\mathrm{sat}} = I'^{\mathrm{sat}}$ in Theorem 3.2.1, item (b), can be a restrictive requirement, in particular in our targeted application for computing orthogonal projections onto rational surfaces. The next result allows us to relax this assumption to the case where the curve component $\mathcal{C}$ of the base locus is a complete intersection.

Theorem 3.2.2. *Assume that* $\dim(\mathcal{B}) = 1$ *and that* $\mathcal{C}$ *has no section in degree* $< (\mathbf{0}, e)$. *Moreover, assume that there exists an homogeneous ideal* $J \subset R$ *generated by a regular sequence* (g_1, g_2) *such that* $I \subset J$ *and* $(I : J)$ *defines a finite subscheme in* $X \times \mathbb{P}^1$. *Denote by* $(\boldsymbol{m}_1, n_1)$, *resp.* $(\boldsymbol{m}_2, n_2)$, *the degree of* g_1, *resp.* g_2. *If* $X = \mathbb{P}^2_k$ *then* $\boldsymbol{m_1}, \boldsymbol{m_2}$ *are degrees, if* $X = \mathbb{P}^1_k \times \mathbb{P}^1_k$ *then* $\boldsymbol{m_1}, \boldsymbol{m_2}$ *are bidegrees such that* $\boldsymbol{m_1} = (m_{1,1}, m_{1,2})$ *and* $\boldsymbol{m_2} = (m_{2,1}, m_{2,2})$. *Set* $\eta := \max(e - n_1 - n_2, 0)$ *and let* p *be a point in* $\mathbb{P}^3$ *such that* $\mathfrak{L}_p$ *is finite. Then,*

$$\operatorname{corank} \mathbb{M}_{(\boldsymbol{\mu},\nu)}(p) = \deg(\mathfrak{L}_p)$$

for any degree $(\boldsymbol{\mu}, \nu)$ *such that*

- *if* $X = \mathbb{P}^2$

$$(\mu, \nu) \quad \in \mathbb{E}(3\delta - 2, e - 1 + \eta) \cup \mathbb{E}(3\delta - 2 - \min\{\boldsymbol{m_1}, \boldsymbol{m_2}\}, 3e - 1). \quad (3.15)$$

- *if* $X = \mathbb{P}^1 \times \mathbb{P}^1$

$$\begin{aligned}(\boldsymbol{\mu}, \nu) \quad &\in \mathbb{E}(3\delta_1 - 1, 2\delta_2 - 1 + \tau_2, e - 1 + \eta) \quad \cup \\ &\mathbb{E}(2\delta_1 - 1 + \tau_1, 3\delta_2 - 1, e - 1 + \eta) \quad \cup \\ &\mathbb{E}(2\delta_1 - 1 + \tau_1, 2\delta_2 - 1 + \tau_2, 3e - 1), \end{aligned} \quad (3.16)$$

where $\tau_i := \delta_i - \min\{2m_{1,i} + m_{2,i}, m_{i,1} + 2m_{2,i}, \delta_i\} \geqslant 0, \ i = 1, 2.$

Proof. The proof of Theorem 3.2.1 applies almost verbatim; the specific properties of this theorem are given in Proposition 3.3.3, as a refinement of Theorem 3.3.1. More details are given in §3.3.3. □

Observe that the lower bounds on the degree $(\boldsymbol{\mu}, \nu)$ given in Theorem 3.2.2 are similar to those given in Theorem 3.3.1 up to shifts in some partial degrees that depend on the defining degrees of the curve $\mathcal{C}$. In addition, we mention that in the case where the base locus $\mathcal{B}$ is finite (including empty), which is the case of a general map Ψ of the form (3.6), Theorem 3.2.1 gives a natural extension of results obtained in [2]. We also emphasize that our motivation to consider maps with one-dimensional base locus comes from congruences of normal lines to rational surfaces that have been introduced in Section 3.1 (see Lemma 3.1.2).

3.3 Vanishing of some local cohomology modules

The goal of this section is to provide results on the vanishing of particular graded parts of some local cohomology modules in order to complete the proofs of Theorem 3.2.1 and Theorem 3.2.2. We first recall and set some notation. Let k be a field and consider the parameterization

$$\begin{array}{rcl} \Psi : X \times \mathbb{P}^1 & \dashrightarrow & \mathbb{P}^3 \\ \xi \times (\bar{t} : t) & \mapsto & (\Psi_0 : \Psi_1 : \Psi_2 : \Psi_3)\,(\xi; \bar{t}, t) \end{array} \quad (3.17)$$

The variety X stands for either $\mathbb{P}^2$ or $\mathbb{P}^1 \times \mathbb{P}^1$, so that $n = 3$ or $n = 4$. We denote by R_X its coordinate ring which is a standard graded polynomial ring. Thus, the polynomials $\Psi_0, \Psi_1, \Psi_2, \Psi_3$ are multi-homogeneous of multi-degree $(\boldsymbol{\delta}, e)$ in the polynomial ring $R := R_X \otimes_k R_1$ where $R_1 = k[\bar{t}, t]$ is the coordinate ring of $\mathbb{P}^1$. We assume that $(\boldsymbol{\delta}, e) \geqslant (\mathbf{1}, 1)$ (otherwise the map is not dominant), where $\mathbf{1} := (1, 1)$ in the case $X = \mathbb{P}^1 \times \mathbb{P}^1$. Let I be the ideal generated by the coordinates of the map Ψ, i.e. $I := (\Psi_0, \Psi_1, \Psi_2, \Psi_3) \subset R$. The base locus $\mathcal{B}$ of Ψ is the subscheme of $X \times \mathbb{P}^1$ defined by I. Without loss of generality, we assume that $\mathcal{B}$ is of dimension at most one.

Theorem 3.3.1. *Take again the notation of §3.2.2 and assume that one of the two following properties holds:*

(a) The base locus $\mathcal{B}$ is finite, possibly empty,

(b) $\dim(\mathcal{B}) = 1$, *$\mathcal{C}$ has no section in degree $< (\mathbf{0}, e)$ and $I^{sat} = I'^{sat}$ where I' is an ideal generated by three general linear combinations of the polynomials $\Psi_0, \ldots, \Psi_3$.*

Then, for any point p in $Spec(R)$ such that $\mathfrak{L}_p$ is finite, possibly empty, we have that $H^i_B(\mathrm{Sym}(I)\otimes_R \kappa(p))_{(\boldsymbol{\mu},\nu)} = 0$ for all integers i and all degree $(\boldsymbol{\mu},\nu)$ satisfying to (3.13) or (3.14).

In order to prove this theorem, we begin with some preliminary results on the control of the vanishing of the local cohomology of the cycles and homology of the Koszul complex associated to the sequence of homogeneous polynomials $\Psi_0,\dots,\Psi_3$.

3.3.1 Some preliminaries on Koszul homology

The properties we prove below hold in a more general setting than the properties of Theorem 3.2.2. In order to state them in this generality we introduce the following notation.

Let S be a standard $\mathbb{Z}^r$-graded polynomial ring; it is the Cox ring of a product of projective spaces $\mathbb{P} := \mathbb{P}^{n_1}\times\cdots\times\mathbb{P}^{n_r}$. We suppose given a sequence $\Psi_0,\dots,\Psi_s$ of homogeneous poynomials in S and we consider their associated Koszul complex $K_\bullet := K_\bullet(\Psi_0,\dots,\Psi_s;S)$. We denote by Z_i and H_i, respectively, the cycles and homology modules of $K_\bullet$.

The irrelevant ideal B of the Cox ring S is the product of the r ideals defined by the r sets of variables. We set $I := (\Psi_0,\dots,\Psi_s)\subseteq S$ and $\mathcal{B} := \mathrm{Proj}(S/I)\subseteq\mathbb{P}$. Recall that, for $i\geqslant 2$, and any S/I-module M with associated sheaf $\mathcal{F}$,

$$H^i_B(M)_{\boldsymbol{\mu}} \simeq H^{i-1}(\mathcal{B},\mathcal{F}(\boldsymbol{\mu}))$$

and in particular $H^i_B(M)=0$ for $i>\dim(\mathcal{B})+1$. We notice that in the setting of (3.17) we have $\dim(\mathcal{B})\leqslant 1$, $s=3$ and either $r=2$ and $(n_1,n_2)=(2,1)$ or $r=3$ and $(n_1,n_2,n_3)=(1,1,1)$.

As in the theory of multigraded regularity, it is important to provide regions in $\mathbb{Z}^r$ where some local cohomology modules of the ring S, or a direct sum of copies of S like K_i, vanish. We first give a concrete application of this idea and then we define regions in the specific case we will be working with. We recall that the support of a graded S-module M is defined as

$$\mathrm{Supp}(M) := \{\boldsymbol{\mu}\in\mathbb{Z}^r \mid M_{\boldsymbol{\mu}}\neq 0\}\subset\mathbb{Z}^r.$$

Proposition 3.3.1. *For any integer i, let $\mathcal{R}_i\subseteq\mathbb{Z}^r$ be a subset satisfying*

$$\forall j\in\mathbb{Z}:\mathcal{R}_i\cap\mathrm{Supp}(H^j_B(K_{i+j}))=\emptyset,$$

i.e. $\mathcal{R}_i$ is assumed to be the complement of the support of the local cohomology modules on the i-th diagonal of the first sheet of row filtered spectral sequences of $\check{\mathscr{C}}^\bullet_B(K_\bullet)$ in $\mathbb{Z}_r$. Then, if $\dim\mathcal{B}\leqslant 1$ the following properties hold for any integer i:

- *For all $\boldsymbol{\mu}\in\mathcal{R}_{i-1}$, $H^1_B(H_i)_{\boldsymbol{\mu}}=0$.*
- *There exists a natural graded map $\delta_i : H^0_B(H_i)\to H^2_B(H_{i+1})$ such that $(\delta_i)_{\boldsymbol{\mu}}$ is surjective for all $\boldsymbol{\mu}\in\mathcal{R}_{i-1}$ and is an isomorphism for all $\boldsymbol{\mu}\in\mathcal{R}_i$.*

In particular,

$$H^0_B(H_i)_{\boldsymbol{\mu}}\simeq H^2_B(H_{i+1})_{\boldsymbol{\mu}} \text{ for all } \boldsymbol{\mu}\in\mathcal{R}_{i-1}\cap\mathcal{R}_i.$$

Proof. We consider the double complex obtained from the Koszul complex $K_\bullet$ by replacing each term by its associated Čech complex with respect to the ideal B, denoted by $\check{\mathscr{C}}^\bullet_B(K_\bullet)$. This double complex gives rise to two spectral sequences that both

converge to the same limit. At the second sheet, the row-filtered spectral sequence is of the following form

$$\begin{array}{ccccccc}
\cdots & H_B^0(H_{i+2}) & & H_B^0(H_{i+1}) & H_B^0(H_i) & H_B^0(H_{i-1}) & \cdots . \\
 & & \overset{\delta_{i+1}}{\searrow} & & \overset{\delta_i}{\searrow} & \overset{\delta_{i-1}}{\searrow} & \\
\cdots & H_B^1(H_{i+2}) & & H_B^1(H_{i+1}) & H_B^1(H_i) & H_B^1(H_{i-1}) & \cdots \\
\cdots & H_B^2(H_{i+2}) & & H_B^2(H_{i+1}) & H_B^2(H_i) & H_B^2(H_{i-1}) & \cdots \\
\cdots & 0 & & 0 & 0 & 0 & \cdots
\end{array}$$

On the other hand, the terms of the column-filtered spectral sequence at the first sheet on the diagonal whose total homology is filtered by $\ker(\delta_i)$, $\operatorname{coker}(\delta_{i+1})$ and $H_B^1(H_{i+1})$ are $H_B^j(K_{i+j})$ for $j \in \mathbb{N}$. It follows that :

$$H_B^1(H_{i+1})_{\boldsymbol{\mu}} = \ker(\delta_i)_{\boldsymbol{\mu}} = \operatorname{coker}(\delta_{i+1})_{\boldsymbol{\mu}} = 0, \forall \boldsymbol{\mu} \in \mathcal{R}_i.$$

□

Remark 3.3.1. *If* $\dim(\mathcal{B}) = 0$ *then* $H_B^2(H_i) = 0$*, for any integer* i*, since* H_i *is a* S/I*-module. Therefore, in this case Proposition 3.3.1 shows that*

$$H_B^0(H_i)_{\boldsymbol{\mu}} = 0, \ \forall \boldsymbol{\mu} \in \mathcal{R}_i \quad \textit{and} \quad H_B^1(H_i)_{\boldsymbol{\mu}} = 0, \ \forall \boldsymbol{\mu} \in \mathcal{R}_{i-1}.$$

We now turn to properties on the cycles of the Koszul complex $K_\bullet(\Psi_0, \ldots, \Psi_s; S)$.

Proposition 3.3.2. *Assume that* $n_i > 0$ *for all integers* i*. Then, for any integer* p *the following properties hold:*

- $H_B^0(Z_p) = H_B^1(Z_p) = 0$,
- $H_B^2(Z_p)_{\boldsymbol{\mu}} \simeq H_B^0(H_{p-1})_{\boldsymbol{\mu}}$ *for all* $\boldsymbol{\mu} \in \mathcal{R}_{p-2}$,
- $H_B^3(Z_p)_{\boldsymbol{\mu}} = 0$ *for all* $\boldsymbol{\mu} \in \mathcal{R}_{p-2} \cap \mathcal{R}_{p-3}$,
- $H_B^4(Z_p)_{\boldsymbol{\mu}} = 0$ *for all* $\boldsymbol{\mu} \in \mathcal{R}_{p-3} \cap \mathcal{R}_{p-4}$.

Proof. We consider the complex

$$\mathcal{C}_\bullet := 0 \to Z_p \hookrightarrow K_p \to K_{p-1} \to \cdots \to K_1 \to K_0 \to 0$$

which is built form the Koszul complex $K_\bullet$. This complex gives rise to the double $\check{\mathscr{C}}_B^\bullet(\mathcal{C}_\bullet)$, which itself gives rise to two spectral sequences that converge to the same limit. The column-filtered spectral sequence has a first sheet in the following form:

$$\begin{array}{ccccc}
H_B^0(Z_p) & 0 & \cdots & 0 & 0 \\
H_B^1(Z_p) & 0 & \cdots & 0 & 0 \\
H_B^2(Z_p) \to & H_B^2(K_p) \to & H_B^2(K_{p-1}) \to & H_B^2(K_{p-2}) \to & \cdots \\
H_B^3(Z_p) \to & H_B^3(K_p) \to & H_B^3(K_{p-1}) \to & H_B^3(K_{p-2}) \to & \cdots \\
H_B^4(Z_p) \to & H_B^4(K_p) \to & H_B^4(K_{p-1}) \to & H_B^4(K_{p-2}) \to & \cdots
\end{array}$$

On the other hand, the row-filtered spectral sequence at the second sheet is of the following form

$$\begin{array}{ccccccc}
0 & 0 & H^0_B(H_{p-1}) & H^0_B(H_{p-2}) & H^0_B(H_{p-3}) & \cdots \\
 & & & \searrow^{\delta_{p-2}} & & \searrow^{\delta_{p-3}} & \\
0 & 0 & H^1_B(H_{p-1}) & H^1_B(H_{p-2}) & H^1_B(H_{p-3}) & \cdots \\
 & & & \searrow^{\delta_{p-2}} & & \searrow^{\delta_{p-3}} & \\
0 & 0 & H^2_B(H_{p-1}) & H^2_B(H_{p-2}) & H^2_B(H_{p-3}) & \cdots \\
0 & 0 & 0 & 0 & 0 & \\
0 & 0 & 0 & 0 & 0 &
\end{array}$$

Comparing these two spectral sequences, and using that they have same abutment, we get the claimed results for $H^0_B(Z_p)$, $H^1_B(Z_p)$, $H^2_B(Z_p)$ and $H^4_B(Z_p)$. For $H^3_B(Z_p)$, we get that $H^3_B(Z_p)_{\boldsymbol{\mu}}$ is filtered by $H^1_B(H_{p-1})_{\boldsymbol{\mu}}$ and $\ker(\delta_{p-2})_{\boldsymbol{\mu}}$ for all $\boldsymbol{\mu} \in \mathcal{R}_{p-2} \cap \mathcal{R}_{p-3}$ and the conclusion follows from Proposition 3.3.1. □

When $s = 3$ and the polynomials $\Psi_0, \ldots, \Psi_3$ are of the same degree $\mathfrak{d}$ (which is equal to $(\boldsymbol{\delta}, e)$ in the setting of (3.17)), the corresponding approximation complex $\mathcal{Z}_\bullet$ to these polynomials is of the form

$$0 \to \mathcal{Z}_3 \to \mathcal{Z}_2 \to \mathcal{Z}_1 \to \mathcal{Z}_0 \to 0,$$

with $\mathcal{Z}_i = Z_i[i\mathfrak{d}] \otimes S(-i)$,. Using the Čech complex construction, we can consider the double complex $\check{\mathscr{C}}^\bullet_B(\mathcal{Z}_\bullet)$ that gives rise to two canonical spectral sequences corresponding to the row and column filtrations of this double complex. The graded pieces of the spectral sequence at the first step for the column filtration are $H^p_B(Z_q)_{\boldsymbol{\mu}+p\mathfrak{d}}$. By Proposition 3.3.2, and under its assumptions, if $\boldsymbol{\mu} \in \mathcal{R}_{-2}$ all these modules vanish except for $(p, q) = (2, 2)$ and for $(p, q) = (2, 1)$. Hence, for $\boldsymbol{\mu} \in \mathcal{R}_{-2}$, $\check{\mathscr{C}}^\bullet_B(\mathcal{Z}_\bullet)_{\boldsymbol{\mu}}$ is quasi-isomorphic to the complex

$$0 \to H^0_B(H_1)_{\boldsymbol{\mu}+2\mathfrak{d}} \otimes S(-2) \to H^0_B(H_0)_{\boldsymbol{\mu}+\mathfrak{d}} \otimes S(-1) \to 0$$

that is in turn isomorphic to

$$0 \to H^2_B(H_2)_{\boldsymbol{\mu}+2\mathfrak{d}} \otimes S(-2) \to H^2_B(H_1)_{\boldsymbol{\mu}+\mathfrak{d}} \otimes S(-1) \to 0$$

for $\boldsymbol{\mu} \in \mathcal{R}_{-1} \subseteq \mathcal{R}_{-2}$ by Proposition 3.3.1, assuming in addition that $\dim(\mathcal{B}) = 1$. Consequently, our next goal is to control the vanishing of the graded parts of $H^2_B(H_1)$ and $H^2_B(H_2)$.

Lemma 3.3.1. *Assume that* $\dim(\mathcal{B}) = 1$ *and that the* $s+1$ *forms* $\Psi_0, \ldots, \Psi_s$ *are of the same degree* $\mathfrak{d}$. *Let* $\mathcal{C}$ *be the unmixed curve component of* $\mathcal{B}$ *and set* $p := s - \dim(\mathbb{P}) + 2$ *and* $\boldsymbol{\sigma} := (s+1)\mathfrak{d} - (n_1 + 1, \cdots, n_r + 1)$. *Then, for all* $\boldsymbol{\mu} \in \mathbb{Z}^r$ *we have*

$$H^2_B(H_p)_{\boldsymbol{\mu}} \simeq H^0(\mathcal{C}, \mathcal{O}_{\mathcal{C}}(-\boldsymbol{\mu} + \boldsymbol{\sigma}))^\vee.$$

In particular, if $\mathcal{C}$ *has no section in degree* $< \boldsymbol{\mu}_0$, *for some* $\boldsymbol{\mu}_0 \in \mathbb{Z}^r$, *then*

$$H^2_B(H_p)_{\boldsymbol{\mu}} = 0 \text{ for all } \boldsymbol{\mu} \in \mathbb{E}((s+1)\mathfrak{d} - (n_1, \cdots, n_r) - \boldsymbol{\mu}_0).$$

Proof. As locally at a closed point $x \in \mathbb{P}$, the Ψ_i's contain a regular sequence of length $s-1$, and of length s unless $x \in \mathcal{C}$, by [9, §1-3] we have the isomorphisms

$$\widetilde{H_p(\boldsymbol{\sigma})} \simeq \widetilde{\mathrm{Ext}_S^{s-1}(S/I, \omega_S)} \simeq \widetilde{\mathrm{Ext}_S^{s-1}(S/I_{\mathcal{C}}, \omega_S)} \simeq \omega_{\mathcal{C}}$$

from which using [66, Proposition 1.3] we deduce that

$$H_B^2(H_p) \simeq \bigoplus_{\boldsymbol{\mu}} H^1(\mathcal{C}, \omega_{\mathcal{C}}(\boldsymbol{\mu} - \boldsymbol{\sigma})). \tag{3.18}$$

Now, applying Serre's duality Theorem [47, Corollary 7.7] we get

$$H^1(\mathcal{C}, \omega_{\mathcal{C}}(\boldsymbol{\mu} - \boldsymbol{\sigma})) \simeq H^0(\mathcal{C}, \mathcal{O}_{\mathcal{C}}(-\boldsymbol{\mu} + \boldsymbol{\sigma}))^{\vee},$$

which concludes the proof. □

Lemma 3.3.2. *In the setting of Lemma 3.3.1, let $s = \dim(\mathbb{P})$ and let I' be an ideal generated by s general linear combinations of the Ψ_i's. If $I^{sat} = I'^{sat}$ then for all $\boldsymbol{\mu} \in \mathbb{Z}^r$ there exists an exact sequence*

$$H^0(\mathcal{C}, \mathcal{O}_{\mathcal{C}}(-\boldsymbol{\mu} - \boldsymbol{\mathfrak{d}} + \boldsymbol{\sigma}))^{\vee} \to H_B^2(H_1)_{\boldsymbol{\mu}} \to H_B^2(S/I)_{\boldsymbol{\mu}-\boldsymbol{\mathfrak{d}}} \to 0.$$

In particular, if $\mathcal{C}$ has no section in degree $< \boldsymbol{\mu}_0$, for some $\boldsymbol{\mu}_0 \in \mathbb{Z}^r$, we have that $H_B^2(H_1)_{\boldsymbol{\mu}} = 0$ for all $\boldsymbol{\mu}$ such that $\boldsymbol{\mu} \in \mathbb{E}(s\boldsymbol{\mathfrak{d}} - (n_1, \cdots, n_r) - \boldsymbol{\mu}_0)$ and $\boldsymbol{\mu} - \boldsymbol{\mathfrak{d}} \in \mathcal{R}_{-2}$.

Proof. We will denote by H_i' the ith homology module of the Koszul complex associated to $I' \subset R$. By [9, Corollary 1.6.13] and [9, Corollary 1.6.21] we have the following graded exact sequence

$$0 \to M \to H_1' \to H_1 \to H_0'(-\boldsymbol{\mathfrak{d}}) \to N \to 0 \tag{3.19}$$

with the property that the modules M and N are supported on $V(B)$, which implies that $H_B^i(M) = H_B^i(N) = 0$ for $i \geqslant 1$.

Now, the column-filtered spectral sequence associated to the double complex obtained by replacing each term in the exact sequence (3.19) by its corresponding Čech complex converges to 0. The first sheet of this spectral sequence has three non zero lines and is of the following form

$$\begin{array}{ccccccccc} H_B^0(M) & \to & H_B^0(H_1') & \to & H_B^0(H_1) & \to & H_B^0(H_0')(-\boldsymbol{\mathfrak{d}}) & \to & H_B^0(N) \\ 0 & \to & H_B^1(H_1') & \to & H_B^1(H_1) & \to & H_B^1(H_0')(-\boldsymbol{\mathfrak{d}}) & \to & 0 \\ 0 & \to & H_B^2(H_1') & \to & H_B^2(H_1) & \to & H_B^2(H_0')(-\boldsymbol{\mathfrak{d}}) & \to & 0 \end{array}$$

which implies that the right part of the bottom line

$$H_B^2(H_1') \to H_B^2(H_1) \to H_B^2(H_0')(-\boldsymbol{\mathfrak{d}}) \to 0$$

is exact. By Lemma 3.3.1, $H_B^2(H_1')_{\boldsymbol{\mu}} \simeq H^0(\mathcal{C}, \mathcal{O}_{\mathcal{C}}(-\boldsymbol{\mu} - \boldsymbol{\mathfrak{d}} + \boldsymbol{\sigma}))^{\vee}$ and, by Proposition 3.3.1, $H_B^2(H_0')(-\boldsymbol{\mathfrak{d}})_{\boldsymbol{\mu}} = H_B^2(S/I)(-\boldsymbol{\mathfrak{d}})_{\boldsymbol{\mu}} = 0$ for $\boldsymbol{\mu} - \boldsymbol{\mathfrak{d}} \in \mathcal{R}_{-2}$. □

Before closing this paragraph, we come back to the setting of Theorem 3.3.1 and provide explicit subsets $\mathcal{R}_i$, as these subsets are key ingredients for proving Theorem 3.3.1. As already mentioned, they can be derived from the known explicit description of the local cohomology of polynomial rings. More precisely, we have $s = 3$ and

the multi-homogeneous polynomials $\Psi_0, \dots, \Psi_3$ are defined in the polynomial ring $S := R = R_X \otimes R_1$ and are of degree $\mathfrak{d} := (\boldsymbol{\delta}, e) \geqslant (\mathbf{1}, 1)$.

We recall the local cohomology module of the rings R_X and R_1 (the coordinate ring of $\mathbb{P}^1$) with respect to the irrelevant ideal B in the setting of (3.17).

- $\check{R}_X := \frac{1}{x_0,\dots,x_r} k[x_0^{-1}, \dots, x_r^{-1}]$ such that $r = 2$, if $X = \mathbb{P}^2$ and $r = 3$, if $X = \mathbb{P}^1 \times \mathbb{P}^1$,
- $\check{R}_1 := \frac{1}{tt} k[\overline{t}^{-1}, t^{-1}]$ (see also §1.6).

Lemma 3.3.3. *We have that $H^i_B(R) = 0$ for all $i \neq 2, 3, 4$. In addition, if $X = \mathbb{P}^2$ then $R_X = k[u, v, w]$ and we have that*

$$H^2_B(R) \simeq R_X \otimes \check{R}_1, \quad H^3_B(R) \simeq \check{R}_X \otimes R_1, \quad H^4_B(R) \simeq \check{R}_X \otimes \check{R}_1.$$

If $X = \mathbb{P}^1 \times \mathbb{P}^1$ then $R_X = R_2 \otimes R_3$, where $R_2 = k[u, \overline{u}]$, $R_3 = k[v, \overline{v}]$, and we have that

$$H^2_B(R) \simeq \bigoplus_{\substack{i=1\dots3,\\ \{i,j,k\}=\{1,2,3\}}} \check{R}_i \otimes R_j \otimes R_k,$$

$$H^3_B(R) \simeq \bigoplus_{\substack{i=1\dots3,\\ \{i,j,k\}=\{1,2,3\}}} R_i \otimes \check{R}_j \otimes \check{R}_k,$$

$$H^4_B(R) \simeq \check{R}_1 \otimes \check{R}_2 \otimes \check{R}_3.$$

Proof. See for instance [5, Lemma 6.7]. □

Using the above lemma, we define the following subsets $\mathcal{R}_i$.

Definition 3.3.1. *With previous notations,*

- *If $X = \mathbb{P}^2$ we set*
  - *$\mathcal{R}_i := \mathbb{Z}^2$ for all integer $i \notin [-4, 2]$,*
  - *$\mathcal{R}_{-4} := \mathbb{E}(-\infty, -1) \cup \mathbb{E}(-2, -\infty)$,*
  - *$\mathcal{R}_{-3} := \mathbb{E}(-2, e-1) \cup \mathbb{E}(\delta - 2, -\infty)$,*
  - *for $i = -2, -1, 0$,*

$$\mathcal{R}_i := \mathbb{E}((i+3)\delta - 2, (i+4)e - 1) \cup \mathbb{E}((i+4)\delta - 2, (i+2)e - 1) \subseteq \mathbb{Z}^2.$$

- *If $X = \mathbb{P}^1 \times \mathbb{P}^1$ we set*
  - *$\mathcal{R}_i := \mathbb{Z}^3$ for all integer $i \notin [-4, 2]$,*
  - *$\mathcal{R}_{-4} := \mathbb{E}(-1, -\infty, -\infty) \cup \mathbb{E}(-\infty, -1, -\infty) \cup \mathbb{E}(-\infty, -\infty, -1)$,*
  - *$\mathcal{R}_{-3} := \mathbb{E}(\delta_1 - 1, -1, -1) \cup \mathbb{E}(-1, \delta_2 - 1, -1) \cup \mathbb{E}(-1, -1, e-1)$,*
  - *for $i = -2, -1, 0$,*

$$\mathcal{R}_i := \bigcup_{(a,b,c)|\{a,b,c\}=\{2,3,4\}} \mathbb{E}((a+i)\delta_1 - 1, (b+i)\delta_2 - 1, (c+i)e - 1) \subseteq \mathbb{Z}^3,$$

- $\mathcal{R}_1 := \mathbb{E}(4\delta_1-1, 4\delta_2-1, 3e-1)\cup\mathbb{E}(4\delta_1-1, 3\delta_2-1, 4e-1)\cup\mathbb{E}(3\delta_1-1, 4\delta_2-1, 4e-1)$,
- $\mathcal{R}_2 := \mathbb{E}(4\delta_1 - 1, 4\delta_2 - 1, 4e - 1)$.

It is straightforward to check that these subsets satisfy to the properties required in Proposition 3.3.1. We notice that $\mathcal{R}_p \subseteq \mathcal{R}_{p-1}$ for all $p \leqslant 1$, but we also emphasize that not all these subsets are the largest possible ones in view of Lemma 3.3.3, as we have restricted ourselves to subsets that fit our needs to prove Theorem 3.3.1 without adding some useless technicalities.

3.3.2 Proof of Theorem 3.3.1

We focus on the difficult case of this theorem, namely the case where the base locus $\mathcal{B}$ is not finite, which corresponds to the item (b) in its statement. If $\mathcal{B}$ is finite, then the proof simplifies as explained in Remark 3.3.1 and gives the same conclusion. In what follows, we take again the notation of (3.17) and Theorem 3.3.1.

We consider the approximation complex $\mathcal{Z}_\bullet$ associated to the sequences of homogeneous polynomials Ψ_0, Ψ_1, Ψ_2 and Ψ_3 (see §1.4 for approximation complex). It inherits the multi-graded structure of R and it has an additional grading with respect to $\mathbb{P}^3 = \mathrm{Proj}(k[x_0, x_1, x_2, x_3])$.

Let $\mathfrak{p}$ be a point in $\mathrm{Spec}(k[x_0, x_1, x_2, x_3])$. The specialization of the approximation complex $\mathcal{Z}_\bullet$ at the point $\mathfrak{p}$ yields the complex $\mathcal{Z}_\bullet^{\mathfrak{p}} := \mathcal{Z}_\bullet \otimes \kappa(\mathfrak{p})$ which is of the form

$$0 \to \mathcal{Z}_3 \otimes \kappa(\mathfrak{p}) \to \mathcal{Z}_2 \otimes \kappa(\mathfrak{p}) \to \mathcal{Z}_1 \otimes \kappa(\mathfrak{p}) \to \mathcal{Z}_0 \otimes \kappa(\mathfrak{p}) \to 0.$$

Notice that $H_0(\mathcal{Z}_\bullet) = \mathrm{Sym}(I)$ and $H_0(\mathcal{Z}_\bullet^{\mathfrak{p}}) = \mathrm{Sym}(I) \otimes \kappa(\mathfrak{p})$.

Now, using the Čech complex construction, we can consider the double complexes $\check{\mathcal{C}}_B^\bullet(\mathcal{Z}_\bullet)$ and $\check{\mathcal{C}}_B^\bullet(\mathcal{Z}_\bullet^{\mathfrak{p}})$ that both give rise to two canonical spectral sequences corresponding to the row and column filtrations of these double complexes. As $\mathcal{C}$, the top unmixed one-dimensional curve component of $\mathcal{B}$, is almost a complete intersection at its generic points, $H_B^i(H_j(\mathcal{Z}_\bullet)) = 0$ for $i > 1$ and $j > 0$. Let $Y \subset \mathrm{Proj}(R/I)$ be the locus where I is not locally an almost complete intersection. Then Y is either empty or of dimension zero. As $\mathcal{Z}_\bullet$ is exact outside of Y, $\mathcal{Z}_\bullet^{\mathfrak{p}}$ is exact outside of $Y \cup \pi_2^{-1}(\mathfrak{p})$. Therefore, it follows from our hypothesis that one also has $H_B^i(H_j(\mathcal{Z}_\bullet^{\mathfrak{p}})) = 0$ for $i > 1$ and $j > 0$. From these considerations, we deduce that the row-filtered spectral sequence of the double complex $\check{\mathcal{C}}_B^\bullet(\mathcal{Z}_\bullet)$ converges at the second sheet and is equal to

$$\begin{array}{ccccc}
0 & H_B^0 H_3(\mathcal{Z}_\bullet) & H_B^0(H_2(\mathcal{Z}_\bullet)) & H_B^0(H_1(\mathcal{Z}_\bullet)) & H_B^0(\mathrm{Sym}(I)) \\
0 & H_B^1 H_3(\mathcal{Z}_\bullet) & H_B^1(H_2(\mathcal{Z}_\bullet)) & H_B^1(H_1(\mathcal{Z}_\bullet)) & H_B^1(\mathrm{Sym}(I)) \\
0 & 0 & 0 & 0 & H_B^2(\mathrm{Sym}(I)) \\
0 & 0 & 0 & 0 & 0
\end{array}$$

On the other hand, the column-filtered spectral sequence of the double complex $\check{\mathscr{C}}_B^\bullet(\mathcal{Z}_\bullet)$ at the first sheet is

$$\begin{array}{cccccc} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 \to H_B^2(\mathcal{Z}_3) & \to H_B^2(\mathcal{Z}_2) & \to H_B^2(\mathcal{Z}_1) & \to H_B^2(\mathcal{Z}_0) & \to 0 & \\ 0 \to H_B^3(\mathcal{Z}_3) & \to H_B^3(\mathcal{Z}_2) & \to H_B^3(\mathcal{Z}_1) & \to H_B^3(\mathcal{Z}_0) & \to 0 & \\ 0 \to H_B^4(\mathcal{Z}_3) & \to H_B^4(\mathcal{Z}_2) & \to H_B^4(\mathcal{Z}_1) & \to H_B^4(\mathcal{Z}_0) & \to 0 & \end{array}$$

It follows that $H_3(\mathcal{Z}_\bullet) = 0$ and $H_B^0(H_2(\mathcal{Z}_\bullet)) = 0$. Moreover, for all degree $(\boldsymbol{\mu}, \nu) \in \mathcal{R}_{-2}$ we have $H_B^i(\mathcal{Z}_j)_{(\boldsymbol{\mu},\nu)} = 0$ unless $i = 2$ and $j \in \{1, 2\}$. Let

$$H_B^0(H_1)_{(\boldsymbol{\mu},\nu)+2(\boldsymbol{\delta},e)} \otimes S[-2] \xrightarrow{\phi_{(\boldsymbol{\mu},\nu)}} H_B^0(H_0)_{(\boldsymbol{\mu},\nu)+(\boldsymbol{\delta},e)} \otimes S[-1] \tag{3.20}$$

be the degree $(\boldsymbol{\mu}, \nu)$ component of the only potentially non zero map of this graded piece of the double complex. Then,

- $H_B^1(\mathrm{Sym}(I))_{(\boldsymbol{\mu},\nu)} = 0$ if and only if $\phi_{(\boldsymbol{\mu},\nu)}$ is surjective,
- $H_B^0(\mathrm{Sym}(I))_{(\boldsymbol{\mu},\nu)} = H_B^1(H_1(\mathcal{Z}_\bullet))_{(\boldsymbol{\mu},\nu)} = 0$ if and only if $\phi_{(\boldsymbol{\mu},\nu)}$ is injective.

The same arguments apply to $\check{\mathscr{C}}_B^\bullet(\mathcal{Z}_\bullet^{\mathfrak{p}})$ and show that for $(\boldsymbol{\mu}, \nu) \in \mathcal{R}_{-2}$:

- $H_B^1(\mathrm{Sym}(I) \otimes \kappa(\mathfrak{p}))_{(\boldsymbol{\mu},\nu)} = 0$ if and only if $\phi_{(\boldsymbol{\mu},\nu)} \otimes \kappa(\mathfrak{p})$ is surjective,
- $H_B^0(\mathrm{Sym}(I) \otimes \kappa(\mathfrak{p}))_{(\boldsymbol{\mu},\nu)} = H_B^1(H_1(\mathcal{Z}_\bullet^{\mathfrak{p}}))_{(\boldsymbol{\mu},\nu)} = 0$ if and only if $\phi_{(\boldsymbol{\mu},\nu)} \otimes \kappa(\mathfrak{p})$ is injective.

Furthermore, for all $(\boldsymbol{\mu}, \nu) \in \mathcal{R}_{-1}$ the map $\phi_{(\boldsymbol{\mu},\nu)}$ identifies with the map

$$H_B^2(H_2)_{(\boldsymbol{\mu},\nu)+2(\boldsymbol{\delta},e)} \otimes S[-2] \longrightarrow H_B^2(H_1)_{(\boldsymbol{\mu},\nu)+(\boldsymbol{\delta},e)} \otimes S[-1]$$

and the conclusion follows from Lemma 3.3.1 and Lemma 3.3.2. Indeed, assume first that $X = \mathbb{P}^2$, then we need to have $(\boldsymbol{\mu}, \nu) \in \mathcal{R}_{-1}$ and Lemma 3.3.1 and Lemma 3.3.2 both require additionally that

$$(\boldsymbol{\mu}, \nu) \in \mathbb{E}(2\delta - 2 - \mu_X, 2e - 1 - \mu_1),$$

where $\boldsymbol{\mu}_0 = (\mu_X, \mu_1)$ is such that the unmixed curve component $\mathcal{C}$ of the base locus has no section in degree $< \boldsymbol{\mu}_0$. Observing that $\mathcal{R}_{-1}$ is precisely the expected region (3.13) to prove our theorem, we must have that

$$\mathcal{R}_{-1} \subseteq \mathbb{E}(2\delta - 2 - \mu_X, 2e - 1 - \mu_1).$$

This latter inclusion holds if $\mu_X \geqslant 0$ and $\mu_1 \geqslant e$. From here, the theorem follows as we assumed that $\mathcal{C}$ has no section in degree $< (\mu_X, \mu_1) = (0, e)$.

Now, consider the case $X = \mathbb{P}^1 \times \mathbb{P}^1$. Similarly, we need to have $(\boldsymbol{\mu}, \nu) \in \mathcal{R}_{-1}$ and both Lemma 3.3.1 and Lemma 3.3.2 require additionally that

$$(\boldsymbol{\mu}, \nu) \in \mathbb{E}(2\delta_1 - 1 - \mu_1, 2\delta_2 - 1 - \mu_2, 2e - 1 - \mu_3),$$

where $\boldsymbol{\mu}_0 = (\mu_1, \mu_2, \mu_3)$. If we impose, as in the case $X = \mathbb{P}^2$, that $\mathcal{R}_{-1}$ is contained in the above region, then we must have $\mu_1 \geqslant \delta_1$, $\mu_2 \geqslant \delta_2$ and $\mu_3 \geqslant e$. In order to have a weaker assumption on the global sections on the curve $\mathcal{C}$, we preferably choose to set $\mu_1 = \mu_2 = 0$ and then restrict $\mathcal{R}_{-1}$ accordingly, which gives the claimed region (3.14).

3.3.3 Residual of a complete intersection curve

The proof of Theorem 3.3.1 completes the proof of Theorem 3.2.1, but it still remains to prove Theorem 3.2.2. For that purpose, we proceed as in the proof of Theorem 3.3.1 but with a different argument to control the vanishing of some graded parts of the module $H^0_B(H_0)$ that appears in (3.20). We maintain the notation of the previous sections.

Proposition 3.3.3. *Let J be an homogeneous ideal in R generated by a regular sequence (g_1, g_2) such that $I \subset J$ and $(I : J)$ defines a finite subscheme in $X \times \mathbb{P}^1$. Denote by $(\boldsymbol{m}_1, n_1)$, resp. $(\boldsymbol{m}_2, n_2)$, the degree of g_1, resp. g_2, and define the integer $\kappa := \min(e, n_1 + n_2)$. Then, $H^0_B(H_0(K_\bullet))_{(\boldsymbol{\mu},\nu)} = 0$ for all $(\boldsymbol{\mu}, \nu)$ satisfying to the following conditions:*

- *if $X = \mathbb{P}^2$,*

$$(\mu, \nu) \quad \in \mathbb{E}(4\delta - 2 - \min\{m_1 + m_2, 2m_1, 2m_2\}, 3e - 1 - \kappa). \tag{3.21}$$

- *if $X = \mathbb{P}^1 \times \mathbb{P}^1$,*

$$\begin{aligned}(\boldsymbol{\mu}, \nu) \in \mathbb{E}(4\delta_1 - 1 - \varepsilon_1, 4\delta_2 - 1 - \varepsilon'_2, 3e - 1 - \kappa) \cup \\ \mathbb{E}(4\delta_1 - 1 - \varepsilon'_1, 4\delta_2 - 1 - \varepsilon_2, 3e - 1 - \kappa)\end{aligned} \tag{3.22}$$

  where for $i = 1, 2$

$$\begin{aligned}\varepsilon_i &:= \min\{2m_{1,i}, m_{1,i} + m_{2,i}, 2m_{2,i}\}, \\ \varepsilon'_i &:= \min\{2m_{1,i} + m_{2,i}, m_{1,i} + 2m_{2,i}, \delta_i + m_{1,i}, \delta_i + m_{2,i}\}.\end{aligned}$$

Proof. Since $I \subset J$, we have the canonical exact sequence

$$0 \to J/I \to R/I \to R/J \to 0$$

and hence, by the associated long exact sequence of local cohomology we deduce that $H^0_B(H_0(K_\bullet))_{(\boldsymbol{\mu},\nu)} = H^0_B(R/I)_{(\boldsymbol{\mu},\nu)} = 0$ if both $H^0_B(R/J)_{(\boldsymbol{\mu},\nu)} = H^0_B(J/I)_{(\boldsymbol{\mu},\nu)} = 0$. Our objective is to analyze these two latter conditions.

Set $\boldsymbol{\sigma} := (\boldsymbol{m}_1 + \boldsymbol{m}_2, n_1 + n_2)$. Since $J = (g_1, g_2)$ is generated by a regular sequence, its associated Koszul complex $K^J_\bullet$,

$$0 \to F_2 = R(-\boldsymbol{\sigma}) \to F_1 = \oplus_{i=1}^2 R(-(\boldsymbol{m}_i, n_i)) \to F_0 = R,$$

is acyclic. Therefore, the two classical spectral sequences associated to the double complex $\check{\mathscr{C}}^\bullet_B(K^J_\bullet)$ shows that $H^0_B(R/J)_{(\boldsymbol{\mu},\nu)} = 0$ for all $(\boldsymbol{\mu}, \nu)$ such that

$$H^2_B(R)_{(\boldsymbol{\mu},\nu)-\boldsymbol{\sigma}} \quad = \quad 0. \tag{3.23}$$

Now, from the inclusion $I \subset J$ the decomposition of the $\Psi_j{}'s$ on the g_1, g_2 gives the 2×4-matrix H such that

$$(\Psi_0\ \Psi_1\ \Psi_2\ \Psi_3) = (g_1\ g_2) \begin{pmatrix} h_{0,1} & h_{1,1} & h_{2,1} & h_{3,1} \\ h_{0,2} & h_{1,2} & h_{2,2} & h_{3,2} \end{pmatrix} = (g_1\ g_2)\, H$$

and which corresponds to the homogeneous map

$$K_1 = R(-(\boldsymbol{\delta}, e))^4 \xrightarrow{H} F_1 = R(-(\boldsymbol{m}_1, n_1)) \oplus R(-(\boldsymbol{m}_2, n_2)).$$

From here, we obtain a finite free graded presentation of J/I, namely

$$F_1' = F_2 \oplus K_1 \xrightarrow{\varphi} F_1 \xrightarrow{(g_1,g_2)} J/I \to 0$$

where the map $\varphi : F_1' \to F_1$ is defined by the matrix

$$\begin{pmatrix} -g_2 & h_{0,1} & h_{1,1} & h_{2,1} & h_{3,1} \\ g_1 & h_{0,2} & h_{1,2} & h_{2,2} & h_{3,2} \end{pmatrix}.$$

Consider the Buchsbaum-Rim complex $C_\bullet$ (We refer the reader to 1.5.4 for an overview of Buchsbaum-Rim complex) associated to φ; it is of the form (see [41, Appendix 2.6] and [22, §2] for the graded version with the appropriate shifting in degrees)

$$\begin{aligned} C_4 = \mathcal{S}_2(F_1^*) \otimes \wedge^5(F_1')(\boldsymbol{\sigma}) \to \quad & C_3 = \mathcal{S}_1(F_1^*) \otimes \wedge^4(F_1')(\boldsymbol{\sigma}) \to \\ & C_2 = \mathcal{S}_0(F_1^*) \otimes \wedge^3(F_1')(\boldsymbol{\sigma}) \to C_1 = F_1' \xrightarrow{\varphi} C_0 = F_1. \end{aligned}$$

The homology of $C_\bullet$ is supported on $\operatorname{ann}_R(J/I) = (I :_R J)$, which is assumed to define a finite subscheme in $X \times \mathbb{P}^1$. Therefore, the spectral sequence corresponding to the row filtration of the double complex $\check{\mathcal{C}}_B^\bullet(K_\bullet)$ abuts at the second sheet, with the term $H_B^0(J/I)$ on the principal diagonal. Comparing it with the spectral sequence corresponding to the column filtration, we deduce that $H_B^0(J/I)_{(\boldsymbol{\mu},\nu)} = 0$ for all $(\boldsymbol{\mu}, \nu)$ such that

$$H_B^2(C_2)_{(\boldsymbol{\mu},\nu)} = H_B^3(C_3)_{(\boldsymbol{\mu},\nu)} = H_B^4(C_4)_{(\boldsymbol{\mu},\nu)} = 0. \tag{3.24}$$

Moreover, from the definition of the free graded R-modules C_i, $i = 2, 3, 4$, we have the graded isomorphisms

$$C_2 \simeq R(-3(\boldsymbol{\delta}, e) + \boldsymbol{\sigma})^4 \oplus R(-2(\boldsymbol{\delta}, e))^6,$$

$$C_3 \simeq \oplus_{i=1}^2 R(-4(\boldsymbol{\delta}, e) + (\boldsymbol{m}_i, n_i) + \boldsymbol{\sigma}) \oplus_{i=1}^2 R(-3(\boldsymbol{\delta}, e) + (\boldsymbol{m}_i, n_i))^4,$$

and

$$C_4 \simeq R(-4(\boldsymbol{\delta}, e) + 2(\boldsymbol{m}_1, n_1)) \oplus R(-4(\boldsymbol{\delta}, e) + \boldsymbol{\sigma}) \oplus R(-4(\boldsymbol{\delta}, e) + 2(\boldsymbol{m}_2, n_2)).$$

From here, using the explicit computation of the local cohomology modules of the polynomial ring R, see Lemma 3.3.3, it is straightforward to check that the claimed regions satisfy both conditions (3.23) and (3.24). Notice that it is assumed that $\boldsymbol{\delta} \geqslant \boldsymbol{m_i} \geqslant 0$ (component-wise if $X = \mathbb{P}^1 \times \mathbb{P}^1$) and $e \geqslant 1$. □

From the proof of Proposition 3.3.3, it is clear that it is possible to list more valid regions than those that are given in the statement where we only provided the regions that are of interest for our application to the computation of orthogonal projections

on rational surfaces. It turns out that listing all the possible regions can be a rather technical and cumbersome task. For instance, in the case $X = \mathbb{P}^2$, we obtain the following list of eight quadrants $Q_{i.j.k}$ for which the expected property hold:

(i) $Q_{1.1.1} = \mathbb{E}(4\delta - 2 - \min\{2m_1, m_1 + m_2, 2m_2\}, 3e - 1 - \min\{n_1 + n_2, e\})$,

(ii) $Q_{1.1.2} = \mathbb{E}(4\delta - 2 - \min\{2m_1, m_1 + m_2\}, 4e - 1 - \min\{2n_2, n_1 + n_2 + e, 2e\})$,

(iii) $Q_{1.2.2} = \mathbb{E}(4\delta - 2 - \min\{2m_1, m_1 + 2m_2, \delta + m_2\}, 4e - 1 - \min\{n_1 + n_2, 2n_2\})$,

(iv) $Q_{1.2.1} = \mathbb{E}(4\delta - 2 - \min\{2m_1, 2m_2\}, 4e - 1 - (n_1 + n_2))$,

(v) $Q_{2.1.1} = \mathbb{E}(4\delta - 2 - \min\{m_1 + m_2, 2m_2\}, 4e - 1 - 2n_1)$,

(vi) $Q_{2.1.2} = \mathbb{E}(4\delta - 2 - (m_1 + m_2), 4e - 1 - \min\{2n_1, 2n_2\})$,

(vii) $Q_{2.2.1} = \mathbb{E}(4\delta - 2 - \min\{2m_2, 2m_1 + m_2, \delta + m_1\}, 4e - 1 - \min\{2n_1, n_1 + n_2\})$,

(viii) $Q_{2.2.2} = \mathbb{E}(4\delta - 2 - \min\{m_1 + 2m_2, 2m_1 + m_2, \delta + m_1, \delta + m_2\},$
$4e - 1 - \min\{2n_1, n_1 + n_2, 2n_2\})$.

For the sake of completeness, we also mention that in the special case where g_1 has degree $(m, 0)$ and g_2 has degree $(0, 1)$, which is important for our targeted application, the union of these eight quadrants is equal to the union of two quadrants $Q_{1.1.1}$ and $Q_{1.2.1}$, which is equal to

$$\mathbb{E}(4\delta - 2, 3e - 2) \cup \mathbb{E}(4\delta - m - 2, 4e - 2).$$

The case $X = \mathbb{P}^1 \times \mathbb{P}^1$ give rise to too many regions so that they cannot be listed exhaustively here.

Proof of Theorem 3.2.2. The proofs of Theorem 3.2.1, and hence Theorem 3.3.1, apply verbatim with the exception of the control of the vanishing of the module $H^0_B(H_0)_{(\boldsymbol{\mu},\nu)}$ that appears in (3.20). Indeed, instead of relying on Lemma 3.3.2 (and Proposition 3.3.1) to obtain regions where this module vanishes, we apply Proposition 3.3.3. As we are still using Lemma 3.3.1, it follows that the claimed region are obtained by intersecting the regions obtained in Theorem 3.2.2 with the additional constrained given by Proposition 3.3.3. To be more precise, if $X = \mathbb{P}^2$ then (μ, ν) must satisfy to (3.13) but also must satisfy the additional condition

$$(\mu, \nu) + (\delta, e) \in \mathbb{E}(4\delta - 2 - \min\{m_1 + m_2, 2m_1, 2m_2\}, 3e - 1 - \kappa).$$

From here one can easily check that the claimed region satisfies these two conditions. The case $X = \mathbb{P}^1 \times \mathbb{P}^1$ follows exactly in the same way. □

3.4 Rings of sections in a product of projective spaces

In order to apply Theorem 3.2.1 and Theorem 3.2.2 in the case of a positive dimensional base locus $\mathcal{B}$, it is necessary to analyze when the curve component of $\mathcal{B}$ has no section in bounded above degrees (see Definition 3.2.2). In this section, we provide classes of curves that satisfy to this property. Hereafter, a curve is understood to be a scheme purely of dimension one.

To begin with, if Z is a product (over the field k) of two schemes we recall the following classical property which is a consequence of the Künneth formula.

Lemma 3.4.1. *Assume Z is the product of two schemes $Z_1 \subseteq \mathbb{P}_1$ and $Z_2 \subseteq \mathbb{P}_2$, where $\mathbb{P}_1$ and $\mathbb{P}_2$ are two products of projective spaces. Then, setting $\mathbb{P} := \mathbb{P}_1 \times \mathbb{P}_2$, for any degree $\boldsymbol{\mu}$ and any degree $\boldsymbol{\nu}$ we have*

$$H^0(Z, \mathcal{O}_Z(\boldsymbol{\mu}, \boldsymbol{\nu})) = H^0(Z_1, \mathcal{O}_{Z_1}(\boldsymbol{\mu})) \otimes_k H^0(Z_2, \mathcal{O}_{Z_2}(\boldsymbol{\nu})).$$

From this property, it is interesting to identify classes of subschemes in a single projective space that have no section in negative degrees, because then this provides new classes of subschemes in product of projective spaces with no section in negative degrees by product extensions.

If Z is a reduced irreducible subscheme in a projective space $\mathbb{P}^n$ (over a field) of positive dimension, then it is well known that $\mathcal{O}_Z(\mu)$ has no non-zero global sections for any integer $\mu < 0$. We show that this result extends to a subscheme of a product of projective spaces.

Let Z be a subscheme in a product of projective spaces $\mathbb{P} := \mathbb{P}^{n_1} \times \cdots \times \mathbb{P}^{n_r}$, $n_i \geqslant 1$ for all i. Let R be the standard multi-graded ring defining $\mathbb{P}$ and let $I \subset R$ be the multi-homogeneous defining ideal of Z. The ring of sections of Z sits in the exact sequence

$$0 \longrightarrow H^0_B(R/I) \longrightarrow R/I \longrightarrow \bigoplus_{\boldsymbol{\mu} \in \mathbb{Z}^r} H^0(Z, \mathcal{O}_Z(\boldsymbol{\mu})) \longrightarrow H^1_B(R/I) \longrightarrow 0$$

where B stands for the ideal generated by $R_{(1,\ldots,1)}$. It shows in particular that Z determines $I_Z = I + H^0_B(R/I)$, the unique ideal saturated with respect to B that defines Z, giving a one to one correspondence between B-saturated multi-graded ideals and subschemes of $\mathbb{P}$.

Proposition 3.4.1. *With the above notation, assume that Z is reduced with only components of positive dimension, then $H^0(Z, \mathcal{O}_Z(\boldsymbol{\mu})) = 0$ for all $\boldsymbol{\mu} < \mathbf{0}$.*

Proof. First, there is a canonical inclusion

$$H^0(Z, \mathcal{O}_Z(\boldsymbol{\mu})) \hookrightarrow \bigoplus_{i=1}^{t} \bigoplus_{\boldsymbol{\mu} \in \mathbb{Z}^r} H^0(Z_i, \mathcal{O}_{Z_i}(\boldsymbol{\mu}))$$

where Z_i, for $i = 1, \ldots, t$, are the irreducible components of Z. Hence we can, and will, assume that Z is reduced and irreducible.

Notice then that the multi-graded ring $A = \oplus_{\boldsymbol{\mu} \in \mathbb{Z}^r} H^0(Z, \mathcal{O}_Z(\mu))$ is a domain, as it sits in the fraction field of A. Let $d := \dim Z$. By Serre duality, for any $\boldsymbol{\mu}$ we have

$$H^0(Z, \mathcal{O}_Z(\boldsymbol{\mu})) \subseteq H^0(Z, \mathcal{O}_{\tilde{Z}}(\boldsymbol{\mu})) \simeq H^d(Z, \omega_Z(-\boldsymbol{\mu})),$$

where $\tilde{Z}$ is the S_2-ification of Z (see [9, p.62]), namely the scheme defined by $\tilde{A} = \mathrm{End}(\omega_A)$, which is itself sitting in the integral closure of A. In fact

$$\tilde{A} = \oplus_{\boldsymbol{\mu}} H^0(Z, \mathcal{O}_{\tilde{Z}}(\boldsymbol{\mu}))$$

as $\tilde{A}$ satisfies S_2.

Now, if $H^0(Z, \mathcal{O}_Z(\boldsymbol{\mu})) \neq 0$ for some $\boldsymbol{\mu} < 0$, let $0 \neq a \in A_{\boldsymbol{\mu}}$. As A is a domain, $a^k \neq 0$ for all $k \geqslant 1$. This implies that $H^d(Z, \omega_Z(-k\boldsymbol{\mu})) \neq 0$ for any k, contradicting Serre vanishing theorem (as $-\mu_1 H_1 ... - \mu_r H_r$ is very ample since $\mu_i < 0$ for all i).

□

3.5 Computing orthogonal projection of points onto a rational surface

In this section, based on our previous results we devise a new method for computing the orthogonal projections of a point $p \in \mathbb{R}^3$ onto a rational surface $\mathcal{S} \in \mathbb{R}^3$. Suppose that $\mathcal{S}$ is parameterized by a rational map $\Phi : X \dashrightarrow \mathbb{P}^3$, as defined in Section 3.1.2 with polynomials of degree $\boldsymbol{d}$, and consider its associated congruence of normal lines $\Psi : X \times \mathbb{P}^1 \dashrightarrow \mathbb{P}^3$, as described in Section 3.1.3. We will compute the orthogonal projections $q_i \in \mathcal{S}$, $i = 1, \ldots, r_p$, of p by means of the matrices $\mathbb{M}_{(\boldsymbol{\mu},\nu)}(\Psi)$, defined in Section 3.2.2. The degree of the defining polynomials of Ψ will be denoted by $(\boldsymbol{\delta}, 1)$; their values in terms of the type of Φ are given in Table 3.2.

In what follows, we assume that $d \geqslant 2$ if $X = \mathbb{P}^2$ and that $d_1 \geqslant 1$ and $d_2 \geqslant 1$ if $X = \mathbb{P}^1 \times \mathbb{P}^1$.

3.5.1 Matrix representations of linear fibers

Consider the family of matrices $\mathbb{M}_{(\boldsymbol{\mu},\nu)}$ associated to Ψ that we introduced in Section 3.2.2. In Section 3.2 it is proved under suitable assumptions that the corank of $\mathbb{M}_{(\boldsymbol{\mu},\nu)}(p)$, p a point in $\mathbb{P}^3$, gives a computational representation of the linear fiber $\mathfrak{L}_p$ of p, providing that $\mathfrak{L}_p$ is finite and $(\boldsymbol{\mu}, \nu)$ satisfies to some conditions. Thus, the matrix $\mathbb{M}_{(\boldsymbol{\mu},\nu)}$ is a universal matrix-based representation of the finite linear fibers of Ψ.

Admissible degrees

In terms of computational efficiency it is important to choose the degree $(\boldsymbol{\mu}, \nu)$ giving the smallest possible matrix $\mathbb{M}_{(\boldsymbol{\mu},\nu)}$. Recall that Φ is defined by polynomials of degree $\boldsymbol{d}$ over X and its congruence of normal lines Ψ is defined by polynomials of degree $(\boldsymbol{\delta}, 1)$ over $X \times \mathbb{P}^1$, as given in Table 3.2 in terms of degree $\mathbf{d}$.

Corollary 3.5.1. *For a general parameterization Φ and a degree $(\boldsymbol{\mu}, \nu)$, the corresponding matrix $\mathbb{M}_{(\boldsymbol{\mu},\nu)}(\Psi)$ yields a matrix representation of the finite linear fibers of Ψ satisfying the following admissible degrees*

- $(\mu, \nu) \in \mathbb{E}(3\delta - 2, 0)$ *if* $X = \mathbb{P}^2$,
- $(\mu_1, \mu_2, \nu) \in \mathbb{E}(3\delta_1 - 1, 2\delta_2 - 1 + d_2, 0)$ *or*
  $(\mu_1, \mu_2, \nu) \in \mathbb{E}(2\delta_1 - 1 + d_1, 3\delta_2 - 1, 0)$ *if* $X = \mathbb{P}^1 \times \mathbb{P}^1$.

Proof. The base locus $\mathcal{B}$ of Ψ is of positive dimension and we denote by $\mathcal{C}$ its unmixed curve component. Since Φ is a general parameterization, Lemma 3.1.2 shows that $\mathcal{C}$ is a complete intersection curve defined by an ideal $J = (g_1, g_2)$ such that $\deg(g_1) = (\boldsymbol{\delta} - \boldsymbol{d}, 0)$ and $\deg(g_2) = (\mathbf{0}, 1)$. Then, from the results given in Section 3.4, we deduce that $\mathcal{C}$ has no section in degree $< (\mathbf{0}, 1)$. Therefore, the assumptions of Theorem 3.2.2 are satisfied. To recover the claimed bounds for the integers $(\boldsymbol{\mu}, \nu)$, we observe that in our setting we have $e - n_1 - n_2 = 1 - 0 - 1 = 0$, which proves the case $X = \mathbb{P}^2$. If $X = \mathbb{P}^1 \times \mathbb{P}^1$, then we have $\tau_i = \delta_i - (\delta_i - d_i) = d_i$, which concludes the proof. □

To be more precise, we remark that we actually proved that the above corollary holds for any parameterization Φ such that its corresponding congruence of normal lines Ψ satisfies the assumptions of Theorem 3.2.1 or Theorem 3.2.2.

From a computational point of view, the fact that ν can be chosen to be equal to zero is extremely important and justifies the theoretical developments in Section

3.3 that lead us to these lower bounds. Indeed, since $\nu = 0$ the cokernel of the corresponding matrix is defined solely on X, and not on $X \times \mathbb{P}^1$. As a consequence, the orthogonal projections can be computed directly on the surface without computing their positions on normal lines (see §3.5.2). In Table 3.3 we give the precise value of the lowest admissible degree, denoted $\boldsymbol{\mu}_0$, in terms of the degree and the type of surface parameterized by Φ.

$\boldsymbol{\mu}_0$	Triangular surface	Tensor-product surface
Non-rational	$6d-8$	$(6d_1-4, 5d_2-3)$ or $(5d_1-3, 6d_2-4)$
Rational	$9d-11$	$(9d_1-7, 7d_2-5)$ or $(7d_1-5, 9d_2-7)$

TABLE 3.3: Lowest admissible degrees $\boldsymbol{\mu}_0$ for building matrix representations depending on the type of surfaces, namely non-rational/rational triangular/tensor-product surfaces.

The above theoretical results lead us to use in practice the matrix $\mathbb{M}_{(\boldsymbol{\mu}_0,0)}$ as a matrix representation of the congruence of normal lines. In what follows we will denote this matrix by $\mathbb{M}$ for simplicity. We recall that its entries are linear forms in $k[x_0, \ldots, x_3]$, so that $\mathbb{M} = \sum_{i=0}^{3} x_i \mathbb{M}_i$ where $\mathbb{M}_i$ are matrices with entries in k similar to the previously defined matrices for curves in Chapter 2.

Computational aspects

The computation of $\mathbb{M}$, equivalently of the matrices $\mathbb{M}_0, \ldots, \mathbb{M}_3$, amounts to solve the linear system formed by the syzygies of $\Psi_0, \ldots, \Psi_3$ of degree $\boldsymbol{\mu}_0$ (see Table 3.3). If the parameterization Φ is given with exact coefficients, i.e. if $k = \mathbb{Q}$, then the computations can be performed over $\mathbb{Q}$, otherwise they are done with floating point arithmetic with 53 bits of precision, which means that there is no certification on the results as we are dealing with numerical approximations in the computations.

In computer-aided design mostly used surfaces are up to degree 3 triangular surface or bi-cubic tensor-product surface, for this reason in this chapter we will give computation time tables only for small degrees. For a general rational cubic surface, $\mathbb{M}$ can be computed in about 28s over $\mathbb{Q}$ and about 0.9s on floating point computations. We notice that this gap in the computation time is expected because of the growth of the heights of matrix entries over $\mathbb{Q}$ (see for instance [57, §1] for more details on this topic). For a general rational bi-quadratic surface, $\mathbb{M}$ is computed in about 31s over $\mathbb{Q}$ whereas it is computed in about 0.16s on floating point computationss. More results are given in Table 3.4 and Table 3.5. We note that these computations have been made with the software MACAULAY2 for the computations over $\mathbb{Q}$, and the software SAGEMATH for the floating point computations, using an Intel(R) Core(TM) i7-6600U CPU @ 2.60GHz on a x86_64 machine with 16 GB of RAM..

	non-rational			rational		
$\deg(\Phi)$	matrix size	time (ms) floating point	time (ms) over $\mathbb{Q}$	matrix size	time (ms) floating point	time (ms) over $\mathbb{Q}$
2	15×7	2	19	36×29	15	266
3	66×51	42	887	153×150	301	28090
4	153×132	314	32473	351×363	2952	–

TABLE 3.4: Size and computation time of $\mathbb{M}$ on floating point arithmetic and over $\mathbb{Q}$ (exact computations) of non-rational and rational triangular surfaces in milliseconds and in given degrees.

	non-rational			rational		
$\deg(\Phi)$	matrix size	time (ms) floating point	time (ms) over $\mathbb{Q}$	matrix size	time (ms) floating point	time (ms) over $\mathbb{Q}$
$(1,1)$	9×5	1	6	9×4	1	7
$(1,2)$	24×16	4	32	30×20	6	125
$(1,3)$	39×27	11	136	51×36	21	1082
$(2,2)$	72×59	44	1460	120×108	157	31182
$(2,3)$	117×98	141	10867	204×188	662	–
$(3,3)$	195×169	575	96704	357×340	3353	–

TABLE 3.5: Size and computation time of $\mathbb{M}$ on floating point arithmetic and over $\mathbb{Q}$ (exact computation) of non-rational and rational tensor-product surfaces in milliseconds and in given degrees.

Finally, we emphasize that the corank of $\mathbb{M}(p)$ for a general point p and a general surface parameterization Φ, in which case the linear fiber $\mathfrak{L}_p$ and the fiber $\mathfrak{F}_p$ coincide, is equal to the Euclidean distance degree of Φ, given in §3.1.2. Thus, our method provides a numerical approach to the computation of the Euclidean distance degree of the algebraic rational surface Φ (see Table 3.6 and Table 3.7).

Complexity estimation in terms of height

According to the Tables 3.6 and 3.7, one can observe that exact computations, i.e. computations over $\mathbb{Q}$, are more time consuming than approximate computations, i.e. computations over floating point numbers. It is because the coefficients that we deal with during exact computations have many digits. In order to estimate the complexity for our computations, in this section an upper bound for heights of matrix $\mathbb{M}_{(\boldsymbol{\mu},0)}$ is given in terms of the height of the polynomials defining the parameterization of the surface Ψ. This section follows from §1.8 and §2.5. Let v be either ∞ or a prime number p. We recall that $\mathbb{Q}_v$ is defined to be the completion of $\mathbb{Q}$ with respect to the absolute value v, also $\mathbb{C}_v$ is defined to be the completion of the algebraic closure of $\mathbb{Q}_v$ with respect to the absolute value v (see §1.8).

Consider the parameterization

$$\begin{array}{rccccc} \psi: & \mathbb{A}^2_{\mathbb{C}_v} & \times & \mathbb{A}_{\mathbb{C}_v} & \to & \mathbb{A}^3_{\mathbb{C}_v} \\ & (s,t) & \times & u & \mapsto & \left(\frac{f_1(s,t,u)}{f_0(s,t,u)}, \ldots, \frac{f_3(s,t,u)}{f_0(s,t,u)}\right) \end{array}$$

of the congruence of normal lines to a given surface (see §3.1), where f_0, f_1, f_2, f_3 are polynomials of degree $\boldsymbol{d}$ over $\mathbb{C}_v$ (one can think them as dehomogenization of

(3.3)). We emphasize that $\boldsymbol{d}$ stands for degree d for triangular surfaces and bidegree (d_1, d_2) for tensor-product surfaces. Let $r_{(\boldsymbol{\mu},1)}$ denotes the number of rows of the intermediary matrix $S_{(\boldsymbol{\mu},1)}$ described in §3.2.2. Then, $r_{(\boldsymbol{\mu},1)}$ is $(d+\mu+1)(d+\mu)$ for triangular surfaces and $2(d_1+\mu_1+1)(d_2+\mu_2+1)$ for tensor-product surfaces. We recall that the height of $S_{(\boldsymbol{\mu},1)}$ is the maximum of the height of f_i for $i = 0, 1, 2, 3$.

Proposition 3.5.1. *Let v denote either ∞ or prime number p. The height of the corresponding matrix representation $\mathbb{M}_{(\boldsymbol{\mu},0)}(\psi)$ has the following upper bound*

$$h_v(\mathbb{M}_{(\boldsymbol{\mu},0)}(\psi)) = \max\{0, r_{(\boldsymbol{\mu},1)} h_v(S_{(\boldsymbol{\mu},1)}) \log((r_{(\boldsymbol{\mu},1)}-1)! h_v(S_{(\boldsymbol{\mu},1)})^{r_{(\boldsymbol{\mu},1)}-1})\}.$$

Proof. See proof of Proposition 2.5.4. □

The experiments on height of $\mathbb{M}_{(\boldsymbol{\mu},\nu)}$ are given in §2.5.1 for similar matrices used in Chapter 2.

3.5.2 Computation of the orthogonal projections

Given a surface parameterization Φ, the matrix $\mathbb{M}$ is computed only once and afterwards it is stored. It provides a universal representation of the finite linear fibers of the corresponding congruence of normal lines Ψ. More precisely, given a point $p = (p_0 : p_1 : p_2 : p_3) \in \mathbb{R}^3$, the cokernel of $\mathbb{M}(p) = \sum_{i=0}^{3} p_i \mathbb{M}_i$ gives a linear representation of the linear fiber $\mathfrak{L}_p$. Thus, if this fiber is finite then classical methods allow to compute the pre-images of p via Ψ by means of numerical linear algebra techniques such as singular value decompositions and eigen-computations (see for instance [39, 15, 32, 30], or [75, 18, 64] in a setting which is similar to the ours). In what follows, we describe the main steps of an algorithm for computing these orthogonal projections in affine space. It is essentially an adaptation to our context of the inversion algorithm [75, §2.4] where similar matrices are used for the computation of the intersection points between 3D lines and trimmed NURBS surfaces.

Input: A point $p \in \mathbb{R}^3$, a matrix representation $\mathbb{M}$ of Ψ and a numerical tolerance ϵ. (We will explain ϵ at Step 2.)

Output: The affine parameters (u_i, v_i) of ϕ, $i = 1, \ldots, l$, of the points q_i that are the orthogonal projections of p onto $\mathcal{S}$.

Step 1: Evaluate $\mathbb{M}$ at the point $p \in \mathbb{R}^3$, and denote by r, respectively c, its number of rows, respectively columns.

Step 2: Compute the approximate cokernel of $\mathbb{M}(p)$ via a singular value decomposition $\mathbb{M}(p) = USV^T$: inspecting the singular values, the numerical rank s of $\mathbb{M}(p)$ is obtained within the tolerance $\epsilon = |\mathbb{M}(p)|_\infty \cdot 10^{-8}$, where $|.|_\infty$ stands for norm infinity, i.e. assume $\mathbb{M}(p) = (m_{ij})_{\substack{1 \leqslant i \leqslant r \\ 1 \leqslant j \leqslant c}}$, then $|\mathbb{M}(p)|_\infty = \max_{1 \leqslant i \leqslant r}\{\sum_{1 \leqslant j \leqslant c} |m_{ij}|\}$ (see [44]). Then, the submatrix K of U corresponding to the last $k := r - s$ rows is a $k \times r$-matrix whose rows form a basis of an approximate cokernel of $\mathbb{M}(p)$. By construction, the columns of K are indexed by the polynomial basis used in the computation the $\mathbb{M}$. For simplicity, we assume that this basis, denoted B, is the following one:

$$\begin{aligned} &\text{if } X = \mathbb{P}^2, B := \{1, u, u^2, \ldots, u^\mu, v, vu, vu^2, \ldots, vu^\mu, \ldots, v^\mu\}, \\ &\text{if } X = \mathbb{P}^1 \times \mathbb{P}^1, B := \{u^{\mu_1}v^{\mu_2}, u^{\mu_1}v^{\mu_2-1}, \ldots, u^{\mu_1}, u^{\mu_1-1}v^{\mu_2}, \ldots, 1\}, \end{aligned} \tag{3.25}$$

where μ or (μ_1, μ_2) are the chosen degrees to build $\mathbb{M}$.

Step 3: The matrix K^T being of rank k, we extract a full-rank $k \times k$ - submatrix M_1 from K^T (for instance by means of a LU-decomposition). Its rows are indexed by an ordered subset B' of B. Then, we choose another submatrix M_2 of K^T corresponding to the rows indexed by the ordered set $u \times B'$ (multiplication is member-wisely). In case $u.B'$ is not contained in B then $\mathbb{M}$ has to be rebuilt by increasing by one the degree with respect to u used to build $\mathbb{M}$ and we go back to step 1.

Step 4: Compute the generalized eigenvalues and eigenvectors of the pencil of matrices $M_1 - uM_2$; these generalized eigenvalues correspond to the v-coordinates of the orthogonal projections of p. Then we filter them to keep those eigenvalues $u_1, \ldots, u_l$ that are real numbers and that are contained in the parameter domain of interest, typically $[0, 1]$ (within a given tolerance).

Step 5: For each generalized eigenvalue u_i, $i = 1, \ldots, l$, extract from its corresponding generalized eigenvector the v-coordinate v_i of a pre-image point of p under Ψ, which is done by computing the ratio of the two first coordinates of this eigenvector (so that the corresponding ratio of monomials in B is equal to u). Finally, if $v_i \in [0, 1]$, check * if the point $\phi(u_i, v_i)$ in an orthogonal projection of p on $\mathcal{S}$ within the tolerance ϵ. If this is the case, then return this point as an orthogonal projection of p on the surface $\mathcal{S}$.

Remark 3.5.1. *Along the algorithm we considered affine parameter values. However, in Step 2, one can consider the homogeneous monomial basis B in corresponding space X, after that in Step 3, chose the send submatrix M_2 of K^T corresponding to the rows indexed by the ordered set $\frac{u}{\bar{u}} \cdot B'$, and at Step 4 consider the pencil of matrices $M_1 - \frac{u}{\bar{u}} M_2$ of which eigenvalues and eigenvectors gives the parameter values $\frac{u}{\bar{u}}$ and $\frac{v}{\bar{v}}$, respectively.*

Example 3.5.1. *Let's consider Example 3.2.2, and compute the orthogonal projections q of the point $p = (1 : 2 : 3)$ in $\mathbb{R}^3$ onto the surface $\mathcal{S}$. At the point p, we have* $\operatorname{corank}(\mathbb{M}_{(2,2,0)})(p) = 5$ *(which is equal to EDdegree, see Table 3.1). The following matrix is the transpose of the cokernel of $(\mathbb{M}_{(2,2,0)}(p)$, i.e. K^T in Step 3 of the above algorithm, with its rows written in biquadratic tensor-product monomial basis. Red with purple and purple with blue rows are M_2 and M_1 respectively, as in Step 4.*

$$\begin{array}{c} \\ u^2v^2 \\ u^2v \\ u^2 \\ uv^2 \\ uv \\ u \\ v^2 \\ v \\ 1 \end{array} \begin{pmatrix} -0.685421414 & 0.0660814878 & 0.0147592847 & -0.537238983 & -0.382857655 \\ 0.0439704446 & 0.514793591 & 0.346591496 & -0.4.22032315 & 0.586864585 \\ 0.360640001 & -0.229700901 & 0.523632427 & -0.2.51154450 & -0.164865982 \\ -0.590414271 & -0.106984279 & 0.301430422 & 0.481345386 & 0.333260359 \\ -0.119454498 & -0.238405369 & 0.123702832 & -0.291896878 & -0.121337251 \\ 0.0335820812 & 0.551596694 & 0.167283215 & 0.0872972013 & -0.183711883 \\ 0.0250897540 & -0.201520074 & 0.668545047 & 0.181893804 & -0.220840750 \\ -0.150984083 & 0.289888760 & 0.156097918 & 0.260172728 & -0.119843326 \\ -0.103879941 & -0.425053866 & 0.000419883743 & -0.211875596 & 0.509078454 \end{pmatrix}$$

Then, there is only one real-valued eigenvalue which is equal to 1.308507934982006. *It corresponds to the parameter value u of the orthogonal projection q of p onto $\mathcal{S}$. The corresponding parameter value of v is computed via the corresponding eigenvector which is* 2.1847721641433284. *Thus, evaluating u and v parameter values into the dehomogenization of the parameterization of the surface $\mathcal{S}$ in (3.11) gives the coordinates of orthogonal projection q in $\mathbb{R}^3$ of p onto $\mathcal{S}$. We find*

$$q = (1.308507934982006, 2.18477216414, 2.8587917129093547).$$

*This last check is necessary because of the existence of 'ghost points' in the cases where the linear fiber is not the fiber.

Example 3.5.2. *Let us consider Example 3.2.2. The rank of $\mathbb{M}_{(2,2,0)}$ at a general point in $\mathbb{P}^3$ is equal to 4, so that the dimension of its cokernel is equal to 5, which is nothing but the Euclidean distance degree of Φ.*

Now, let $p := (0 : 0 : 2) \in \mathbb{R}^3$. The computation of the cokernel of $\mathbb{M}_{(2,2,0)}(p)$ returns the following matrix

$$K := \begin{pmatrix} 2 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & -1 & 0 & 1 & 0 & 0 & 0 \\ -1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & -1 & 0 & 2 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

whose columns are indexed by the monomial basis $B := \{u^2v^2, u^2v, u^2, uv^2, uv, u, v^2, v, 1\}$. According to the shape of B, we define M_1 as the first 5 rows of K^T (red and purple ones) and M_2 as the last 5 rows, except the very last one (purple and blue ones), of K^T. Then solving for the eigenvectors of the pencil (M_2, M_1), we get the following list of eigenvalues

$$\{0, 1.73205081i, -1.73205081i, 1, -1\}$$

and their corresponding eigenvectors sorted by columns (with tolerance 10^{-18})

$$\begin{bmatrix} 0 & 0.577498923 & 0.577498923 & 0.492765476 & 0.450536889 \\ 0 & -1.22439500 \cdot 10^{-16} + 0.3.33419159\mathbf{i} & -1.22439500 \cdot 10^{-16} - 0.333419159\mathbf{i} & 0.492765476 & -0.450536889 \\ 0 & -0.577498923 - 3.59905499 \cdot 10^{-17}\mathbf{i} & -0.577498923 + 3.59905499 \cdot 10^{-17}\mathbf{i} & 0.492765476 & 0.450536889 \\ 0 & 8.84372488 \cdot 10^{-17} - 0.333419159\mathbf{i} & 8.84372488 \cdot 10^{-17} + 0.333419159\mathbf{i} & 0.492765476 & -0.4.50536889 \\ 1 & 0.208118837 + 0.25949926\mathbf{i} & 0.208118837 - 0.25949926\mathbf{i} & 0.169495558 & 0.433665823 \end{bmatrix}$$

From here, we see that there are three real orthogonal points whose u-parameter values are $u_1 = 0.0$, $u_2 = 1.0000000000000002$ and $u_2 = -1.0000000000000007$. Then, using the basis B and the first two rows of the eigenvectors matrix, we deduce their v-parameter values: $v_1 = 0$, $v_2 = 0.9999999999999996$ and $v_3 = -0.9999999999999996$. The real orthogonal projections of p on the Segre surface are then obtained as $\Phi(u_i, v_i)$, $i = 1, 2, 3$. These computations are illustrated (in SageMath*) with Figure 3.3.*

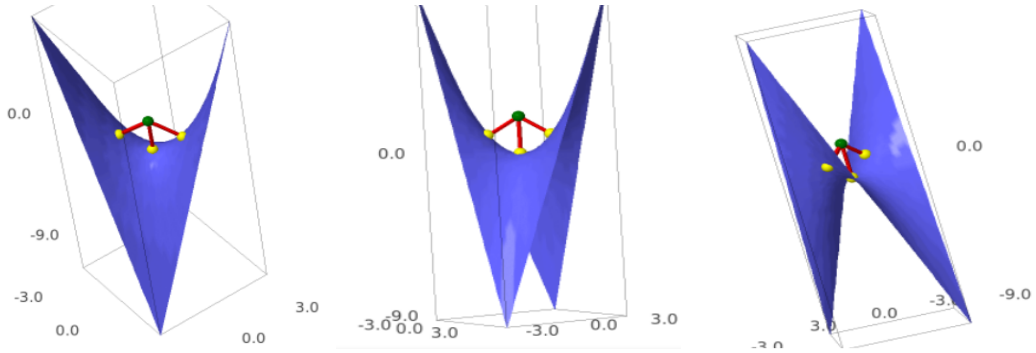


FIGURE 3.3: Orthogonal projections (yellow points) of the affine point $(0, 0, 2)$ (green point) on the Segre variety.

3.5.3 Experiments

The algorithm described in Section 3.5.2 has been implemented in the software SageMath. In Table 3.7, respectively Table 3.6, we report on the computation time to

inverse a general point of a general non-rational and rational tensor-product, respectively triangular surfaces. All the computations are done approximately, over the real numbers $\mathbb{R}$, and it is assumed that the matrix representation $\mathbb{M}$ has already been computed and stored.

	non-rational			rational		
$\deg(\Phi)$	size	EDdeg	time (ms)	size	EDdeg	time (ms)
2	15×7	9	3	36×29	13	3
3	66×51	25	5	153×150	39	13
4	153×132	49	18	351×363	79	113

TABLE 3.6: Size and computation time in milliseconds of the inversion of $\mathbb{M}(p)$ of non-rational and rational triangular surfaces.

	non-rational			rational		
$\deg(\Phi)$	size	EDdeg	time (ms)	size	EDdeg	time (ms)
$(1,1)$	9×5	5	1	9×4	6	1
$(1,2)$	24×16	11	2	30×20	14	2
$(1,3)$	39×27	17	3	51×36	22	3
$(2,2)$	72×59	25	4	120×108	36	10
$(2,3)$	117×98	39	14	204×188	58	29
$(3,3)$	195×169	61	76	357×340	94	137

TABLE 3.7: Size and computation time in milliseconds of the inversion of $\mathbb{M}(p)$ of non-rational and rational tensor-product surfaces.

The method we introduced is particularly well adapted to problems where intensive orthogonal projection computations have to be performed on the same geometric model, thanks to the pre-computation of the matrix representation $\mathbb{M}$. Indeed this matrix allows to rely on powerful and robust numerical tools of linear algebra; see for instance Figure 3.4 where orthogonal projections are close to the self-intersection locus of the surface.

Finally, we mention that the method proposed by Thomassen et al. [78] is also based on the use of congruences of normal lines, but on the algebraic side they use high degree equations of the Rees algebra associated to the defining polynomials of the congruence map (called *moving surfaces*) (see [78, §3]), which make the computations heavy in terms of time and memory. In our approach, we overcome this difficulty using the results in Section 3.3 that allows us to use low degree syzygies, i.e. equations of the above Rees algebra that are *linear* in the space variables (i.e. *moving planes*, and not moving surfaces of high degree in the space variables).

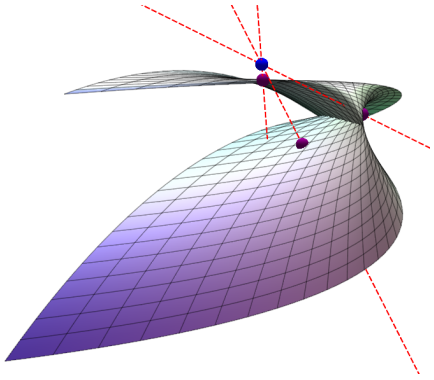


FIGURE 3.4: Orthogonal projections of a point onto a non-rational bi-quadratic surface patch close to its self-intersection locus.

3.5.4 Comparison with homotopy continuation

In this section, we compare our method for computing orthogonal projections of a point onto a rational algebraic surface with the method of homotopy continuation. In the experiments of this section, we only consider tensor-product surfaces. Indeed we have the similar results for triangular surfaces. Suppose given a surface parameterization φ as in (3.1) and a point $p = (p_x, p_y, p_z)$ in $\mathbb{R}^3$. We consider two partial derivatives F_1, F_2 of the square distance function between p and the surface $\mathcal{S}$, denoted by $\mathrm{dist}(p, \varphi(u, v))$, more precisely

$$\begin{aligned} F_1 = &\quad (f_1 - p_x f_0)\tfrac{\partial}{\partial u}(\tfrac{f_1}{f_0}) + (f_2 - p_x f_0)\tfrac{\partial}{\partial u}(\tfrac{f_2}{f_0}) + (f_3 - p_x f_0)\tfrac{\partial}{\partial u}(\tfrac{f_3}{f_0}), \\ F_2 = &\quad (f_1 - p_x f_0)\tfrac{\partial}{\partial v}(\tfrac{f_1}{f_0}) + (f_2 - p_x f_0)\tfrac{\partial}{\partial v}(\tfrac{f_2}{f_0}) + (f_3 - p_x f_0)\tfrac{\partial}{\partial v}(\tfrac{f_3}{f_0}) \end{aligned} \tag{3.26}$$

We choose f_0, f_1, f_2, f_3 as dense polynomials over $\mathbb{R}$ such that all are of the same given degree. We use PHCPY interface of SAGEMATH for solving $F_1 = 0$ and $F_2 = 0$ via a homotopy method which is based on the work [81] (see [70] for details about PHCPY interface). We used this interface online through a JupyterHub server (see [70]) and compared the timing of the inversion of $\mathbb{M}_\nu$ for the smallest possible matrix given in Table 3.3 and the timing of homotopy method over 50 examples for each given degree of such randomly choosen tensor-product surfaces. For this comparison, we supposed that for each example, the corresponding $\mathbb{M}_\nu$ was pre-computed. We observed that inversion is approximately 27 times faster than homotopy method for bi-cubic surfaces and almost 92 times faster for bi-quartic surfaces.

Let us denote the bidegre of F_1 and F_2 by (d_{1_1}, d_{1_2}) and (d_{2_1}, d_{2_2}) respectively. Then, the corresponding bi-homogeneous Bézout bound is given by

$$d_{1_1} d_{2_2} + d_{1_2} d_{2_1},$$

(see [71, 65]). The homotopy method of PHCPY interface computes exactly the Bézout bound number of solutions which is more than the Euclidean distance degree. Thus it computes more points than the orthogonal projections (for rational tensor-product surfaces see Table 3.8).

	non-rational			rational		
$\deg(\Phi)$	Bézout	EDdeg	$\deg(F_1), \deg(F_2)$	Bézout	EDdeg	$\deg(F_1), \deg(F_2)$
$(1,1)$	5	5	(1,2),(2,1)	13	6	(2,3),(3,2)
$(1,2)$	11	11	(1,4),(2,3)	28	14	(2,6),(3,5)
$(1,3)$	17	17	(1,6),(2,5)	43	22	(2,9),(3,8)
$(2,2)$	25	25	(3,4),(4,3)	61	36	(5,6),(6,5)
$(2,3)$	39	39	(3,6),(4,5)	94	58	(5,9),(6,8)
$(3,3)$	61	61	(5,6),(6,5)	145	94	(8,9),(9,8)

TABLE 3.8: Bi-homogeneous Bézout bound of F_1 and F_2 in (3.26) of tensor-product surfaces in given degrees.

3.6 Orthogonal projection onto a rational space curve

For the sake of completeness, in this section we apply our method for the computation of orthogonal projection of points onto a rational space curve. In this case, it can be performed simply because it relies on the solving of a univariate polynomial, which can be done efficiently. Indeed, suppose given a parameterization of a rational space curve $\mathcal{C}$ of degree d

$$\begin{array}{rccc} \phi : \mathbb{A}^1 & \dashrightarrow & \mathbb{A}^3 & \\ t & \longmapsto & \left(\dfrac{f_1(t)}{f_0(t)}, \dfrac{f_2(t)}{f_0(t)}, \dfrac{f_3(t)}{f_0(t)} \right). \end{array} \tag{3.27}$$

The polynomials $f_i(t)$ are assumed to be of degree (at most) d and the map ϕ is assumed to be birational onto $\mathcal{C}$. A tangent vector to the curve $\mathcal{C}$ at the point $\phi(t)$, if it is nonsingular and well-defined, is given by

$$\tau(t) = (\delta_1(t), \delta_2(t), \delta_3(t))$$

where, for all $i = 1, 2, 3$,

$$\delta_i(t) \quad := \det \begin{pmatrix} f_0(t) & f_i(t) \\ f_0'(t) & f_i'(t) \end{pmatrix} = f_0(t) f_i'(t) - f_i(t) f_0'(t), \tag{3.28}$$

is a polynomial of degree at most $2d-2$ (the leading coefficients of degree $2d-1$ cancel). Thus, the orthogonal projection of a point $p = (x, y, z) \in \mathbb{R}^3$ onto the curve $\mathcal{C}$ correspond to the values of the parameter t that are solutions of the equation

$$(p - \phi(t)) \,.\tau(t) v \quad = \quad (x\delta_1 + y\delta_2 + z\delta_3) f_0 - \sum_{i=1}^{3} \delta_i f_i = 0, \tag{3.29}$$

which is a polynomial equation of degree at most $3d-2$ (notice that singular points that are local to the parameter, i.e. such that $\tau(t) = 0$, are solutions of (3.29)). In what follows, we will show the syzygy-based approach we developed for the computation of orthogonal projections onto a surface may be applied to space curves and that amounts essentially to solve this same univariate polynomial by means of eigen-computations.

We keep the same notation as (3.28). The normal plane to the curve $\mathcal{C}$ at the point $\phi(t)$ is generated by two vectors of rational functions; we choose two such vectors and

denote them by

$$\eta_1(t) = (p_1(t), p_2(t), p_3(t)),\ \ \eta_2(t) = (q_1(t), q_2(t), q_3(t)).$$

Standard candidates for these vectors are two independent linear combinations of the three canonical vectors

$$\begin{pmatrix} \delta_2(t) \\ -\delta_1(t) \\ 0 \end{pmatrix}, \begin{pmatrix} \delta_3(t) \\ 0 \\ -\delta_1(t) \end{pmatrix}, \begin{pmatrix} 0 \\ \delta_3(t) \\ -\delta_2(t) \end{pmatrix}.$$

Except for finitely many values of $t \in \mathbb{A}^1$, $\eta_1(t)$ and $\eta_2(t)$ chosen as above will generate all the normal planes to $\mathcal{C}$ at the point $\phi(t)$, $t \in [0,1]$. But instead of looking at these Koszul-type syzygies of the tangent vector $\tau(t)$, a more interesting choice is to look at syzygies of smaller degree. To be more precise, assume for simplicity that $\delta_1(t), \delta_2(t)$ and $\delta_3(t)$ have no common factor. By the Hilbert-Burch Theorem [41, Theorem 20.15] there exist two vectors of polynomials $(p_1(t), p_2(t), p_3(t))$ and $(q_1(t), q_2(t), q_3(t))$ and a nonzero constant $c \in k \setminus \{0\}$ such that

$$\begin{pmatrix} p_1 \\ p_2 \\ p_3 \end{pmatrix} \wedge \begin{pmatrix} q_1 \\ q_2 \\ q_3 \end{pmatrix} = c \begin{pmatrix} \delta_1 \\ \delta_2 \\ \delta_3 \end{pmatrix}.$$

These two vectors generate the first syzygy module of $\delta_1(t), \delta_2(t)$ and $\delta_3(t)$. Moreover, if we define μ_1 to be the maximum of the degree of p_1, p_2, p_3 and μ_2 to be the maximum of the degree of q_1, q_2, q_3 then $\mu_1 + \mu_2 = 2d - 2$ which is the degree of the δ_i's for $i = 1, 2, 3$. Without loss of generality, we will assume that $\mu_1 \leqslant \mu_2$.

As a consequence of the above discussion, the normal plane at a nonsingular and well-defined point $\phi(t)$ of $\mathcal{C}$, can be generated by both vectors

$$\eta_1(t) = \begin{pmatrix} p_1(t) \\ p_2(t) \\ p_3(t) \end{pmatrix}, \quad \eta_2(t) \begin{pmatrix} q_1(t) \\ q_2(t) \\ q_3(t) \end{pmatrix}$$

and hence the family of normal planes to the curve $\mathcal{C}$ can be parameterized by the rational map

$$\begin{array}{rcl} \psi : \mathbb{A}^2 \times \mathbb{A}^1 & \dashrightarrow & \mathbb{A}^3 \\ (u, v) \times t & \mapsto & \phi(t) + u.\eta_1(t) + v.\eta_2(t). \end{array} \tag{3.30}$$

It follows that the orthogonal projection of a point $p \in \mathbb{R}^3$ onto $\mathcal{C}$ can be obtained from its pre-images under ψ. In order to apply our syzygy-based approach to solve this inversion problem, we first need to homogenize the parameterization ψ. For that purpose, we introduce some notation: we denote by $F_i(\bar{t}, t)$ the homogenization of $f_i(t)$ of degree d, by $P_j(\bar{t}, t)$ the homogenization of $p_j(t)$ of degree μ_1 and by $Q_j(\bar{t}, t)$ the homogenization of $q_j(t)$ of degree μ_2. In addition, we also define Δ_i to be the homogenization of δ_i of degree $2d - 2$ and we set $D := \max\{d, \mu_2\}$.

$$\begin{array}{rcl} \Psi : \mathbb{P}^2 \times \mathbb{P}^1 & \dashrightarrow & \mathbb{P}^3 \\ (w : u : v) \times (\bar{t} : t) & \mapsto & (\Psi_0 : \Psi_1 : \Psi_2 : \Psi_3) \end{array} \tag{3.31}$$

where

$$\Psi_0 := w\bar{t}^{D-d}F_0, \quad \Psi_i := w\bar{t}^{D-d}F_i + u\bar{t}^{D-\mu_1}P_i + v\bar{t}^{D-\mu_2}Q_i, \quad \text{for } i = 1,2,3.$$

Thus, the Ψ_i's are bi-homogeneous polynomials of degree $(1, D)$.

Applying Theorem 3.2.1 and Theorem 3.2.2, we see that the orthogonal projections of points in $\mathbb{P}^3$ onto the curve $\mathcal{C}$ can be computed from the matrix representation of the parameterization Ψ of normal planes to the curve $\mathcal{C}$, denoted by $\mathbb{M}(\Psi)_{(\mu,\nu)}$, under some hypothesis.

Lemma 3.6.1. *For a general curve parameterization ϕ, the curve component of the base locus $\mathcal{B}$ of its corresponding congruence of normal planes Ψ as defined in (3.31), is at most one dimensional and given by*

(a) the ideal $(w, \bar{t})$, if $\mu_2 = d - 1$,

(b) the ideal $(w, u\bar{t}^2, v)$, if $\mu_2 = d$,

(c) the ideal $(w, v, \bar{t}^{\mu_2-d})$, if $\mu_2 > d$.

We recall that $\mu_2 \geqslant \mu_1$, $\mu_1 + \mu_2 = 2d - 2$ and $D = \max\{d, \mu_2\}$.

Proof. Analogous to proof of Lemma 3.1.2:

(a) If $\mu_2 = d - 1$ then $\Psi_0 = wF_0$ and $\Psi_i = wF_i + uP_i + vQ_i\bar{t}$, for $i = 1, 2, 3$.

(b) If $\mu_2 = d$, then $\Psi_0 = wF_0$ and $\Psi_i = wF_i + uP_i\bar{t}^2 + vQ_i$, for $i = 1, 2, 3$. Thus, the ideal $(w, u\bar{t}^2, v)$ defines a point.

(c) If $\mu_2 > d$, then $\Psi_0 = wF_0\bar{t}^{\mu_2-d}$ and $\Psi_i = wF_i\bar{t}^{\mu_2-d} + uP_i\bar{t}^{\mu_2-\mu_1} + vQ_i$, for $i = 1, 2, 3$.

□

Lemma 3.6.2. *Let Ψ be a general parameterization of degree $(1, D)$ over $\mathbb{P}^2 \times \mathbb{P}^1$ and let p be a point in $\mathbb{P}^3$ such that the linear fiber $\mathfrak{L}_p$ is finite.*

1. *Assume that we are in one of the two following cases:*

   (a) The base locus $\mathcal{B}$ is finite, possibly empty,

   (b) $\dim(\mathcal{B}) = 1$, the unmixed component of the base locus $\mathcal{C}$ has no section in degree $< (0, D)$ and $I^{sat} = I'^{sat}$ where I' is an ideal generated by three general linear combinations of the polynomials $\Psi_0, \Psi_1, \Psi_2, \Psi_3$.

   Then, we consider any degree (μ, ν) such that

$$(\mu, \nu) \quad \in \mathbb{E}(1, D-1) \cup \mathbb{E}(0, 3D-1). \tag{3.32}$$

2. *We are in the case: $\mathcal{C}$ having no section in degree $< (0, D)$. Assume that,*

   (a) if $\mu_2 > d$, then $I \subset J$ where $J = (v, \bar{t}^{\mu_2-d})$,

   (b) if $\mu_2 = d - 1$, then $I \subset J$ where $J = (w, \bar{t})$.

   such that $(I : J)$ defines a finite subscheme in $\mathbb{P}^2 \times \mathbb{P}^1$. Then, we consider any degree (μ, ν) such that

$$(\mu, \nu) \quad \in \mathbb{E}(1, D-1) \cup \mathbb{E}(0, 4D-1). \tag{3.33}$$

   ($D = \mu_2$ if $\mu_2 > d = \deg(F_i)$ for $i = 0, \ldots, 3$ or $D = d$ if $\mu_2 = d - 1$).

Then, for any such degree (μ, ν) *we have*

$$\operatorname{corank} \mathbb{M}_{(\boldsymbol{\mu},\nu)}(p) = \deg(\mathfrak{L}_p).$$

Proof. The proof of the case 1. is the same as the proof of Theorem 3.3.1. Case 2. follows from

(a) if $\mu_2 > d$, then $(g_1, g_2) = (v, \bar{t}^{\mu_2 - d})$, and $m_1 = 1, n_1 = 0, m_2 = 0, n_2 = \mu_2 - d$,

(b) if $\mu_2 = d - 1$, then $(g_1, g_2) = (w, \bar{t})$, and $m_1 = 1, n_1 = 0, m_2 = 0, n_2 = 1$.

We also notice that if $\mu_2 = d$, the base locus $\mathcal{B}$ is not one dimensional (see Lemma 3.6.1.). Then, for the parameterization Ψ of degree $(1, D)$ Theorem 3.2.2 becomes

$$\mathbb{E}(1 + \eta, D - 1) \cup \mathbb{E}(0, 3D - 1 + D - \min\{n_1, n_2\}),$$

where $\eta = \max\{1 - m_1 - m_2, 0\}$, since degree n_1, n_2 are over the curve parameters, and degrees m_1, m_2 are over the parameters of normal plane to the curve. □

By definition, such a matrix $\mathbb{M}(\Psi)_{(\mu,\nu)}$ (as in Lemma 3.6.2) is filled with those syzygies of the polynomials $\Psi_0, \ldots, \Psi_3$ that are independent of the variables (w, u, v). The following proposition shows that these syzygies are actually closely connected to the equation (3.29).

Proposition 3.6.1. *The syzygies of* $\Psi_0, \ldots, \Psi_3$ *that only depend on the variables* $\bar{t}, t$ *form a free* $k[\bar{t}, t]$*-module of rank 1. Moreover, it is generated in degree* $3d - 2$ *by the vector*

$$(F_1\Delta_1 - F_2\Delta_2 + F_3\Delta_3, -F_0\Delta_1, -F_0\Delta_2, -F_0\Delta_3) \tag{3.34}$$

providing its four polynomial coordinates do not have a common factor.

Proof. From the definition of the parameterization Ψ, the 4-uple g_0, g_1, g_2, g_3 of homogeneous polynomials in $R := k[\bar{t}, t]$ of the same degree is a syzygy of Ψ_0, Ψ_1, Ψ_2 and Ψ_3 if and only if it satisfies to the matrix equality

$$\begin{pmatrix} F_0(\bar{t},t) & F_1(\bar{t},t) & F_2(\bar{t},t) & F_3(\bar{t},t) \\ 0 & P_1(\bar{t},t) & P_2(\bar{t},t) & P_3(\bar{t},t) \\ 0 & Q_1(\bar{t},t) & Q_2(\bar{t},t) & Q_3(\bar{t},t) \end{pmatrix} \times \begin{pmatrix} g_0(\bar{t},t) \\ g_1(\bar{t},t) \\ g_2(\bar{t},t) \\ g_3(\bar{t},t) \end{pmatrix} = 0.$$

This matrix of size 3×4 defines a graded map $\varphi : R^4 \to R(d) \oplus R(\mu_1) \oplus R(\mu_2)$ and it is known that its kernel is a free R-module of rank 1 providing the ideal generated by its 3×3 minors has depth at least 2, and in this latter case these minors generate this kernel. This proves the proposition since these minors are precisely the coordinates of the vector (3.34). □

To conclude, we notice that for a general choice of curve parameterization one has $\mu_1 = \mu_2 = d - 1 = \frac{\deg(\delta_i)}{2}$ for $i = 1, 2, 3$ ($\deg(\delta_i) = 2d - 2$, for a general curve parameterization of degree d (see (3.28))); in this case $D = d$ (see (b) in the proof of Lemma 3.6.1) and $\mathbb{M}_{\nu_0}(\Psi)$ is expected to be a rank 2 matrix composed of two columns and $3d$ rows, with a kernel of dimension at most $3d - 2$ which is equal to degree of the equation in (3.29).

As a consequence, the method we introduced in §3.5.2 for computing the orthogonal projections of points onto a rational algebraic surface can be seen as an extension of the classical approach consisting of solving (3.29) for rational curves.

The direct generalization of (3.29) leads to solve bivariate polynomial system. As we observed in §3.5.4, although our approach requires more sophisticated developments, it allows to reduce remarkably the computation time which is interesting for practical applications in CAGD.

APPENDIX A

Distance between a circle and a line in space

This appendix describes the algorithms computing the distance between a circle and a line, also between an arc of a circle and a line segment in space that I experimented and implemented during my 3-month secondment at Missler Software. These problems were chosen to improve some existing algorithms in their CAD/CAM software called TopSolid. I prepared a module corresponding to these computations, based on C# programming language. The methods which are described in this appendix are implemented in C# and integrated into their interface. I changed algorithmically the existing approches in order to consider all critical points of corresponding distance problem and improve the accuracy together with the computation time. The distance computation algorithms in TopSolid work only after if there is no detected intersection between the line and the circle which we consider. For this reason, my algorithms exclude the case of intersection.

In §A.1, we give the notations of some geometric objects such as line, circle, arc of a circle in space as they are used in TopSolid software. In §A.3, the algorithm that I implemented for distance problem between a circle and a line in space is explained. In order to improve the computation time, the problem is studied in three cases : the line is perpendicular to the plane where the circle is located, the line is in the same plane as the circle, and the general case. Also the corresponding algorithm is given (see Algorithm 3). Mainly, the existing algorithms and the new approach write the same distance function in different ways. The improvements are with respect to the consideration of all critical points and the fact that the computation only depends on the parameter value of the line. We chose to use the parameter value of line because the rational parameterization of the circle given in Notation A.1.2 causes distorsion around the point $(-1, 0, 0)$ that it cannot cover. The more we approach to this point, the more we have numerical instability. This is because the limit of the derivative of the coordinates of the parameterization of the unit circle given in Notation A.1.2 approaches fast to zero, while the parameter value of the parameterization is going to $-\infty$. Our choice of using the parameter value of line allows us to avoid any possible rotations to stay away from the point $(-1, 0, 0)$ contrarily to the existing algorithm. We consider the real valued critical points of this distance problem according to a root classification theorem recalled in §A.3.4. In §A.4, the new algorithm that I implemented for the second problem on distance between an arc of a circle and a line segment in space is given and explained (see Algorithm 4). Finally, the observations mainly on tolerance choices, problems of existing algorithms in TopSolid, comparisons

of the new algorithms that I implemented with the previous algorithms in TopSolid for different cases are explained and illustrated with several examples.

A.1 Notations

We emphasize that existing methods in TopSolid software do not consider line segments, they consider only entire lines.

Notation A.1.1. *The origin in space is denoted by $\mathcal{O}$, i.e. $\mathcal{O} = (0,0,0)$ in $\mathbb{R}^3$. The coordinates of $\mathbb{R}^3$ are denoted by (x,y,z). The plane of $z=0$ will be called the XY-plane.*

Notation A.1.2. *A circle $\mathcal{C}$ in $\mathbb{R}^3$ is given by its center O and radius r and its plane. A parameterization of the unit circle centered at $\mathcal{O}$ with respect to the cartesian coordinates $(\vec{e_i}, \vec{e_j}, \vec{e_k})$ in XY-plane is given by*

$$\left(\frac{1-u^2}{1+u^2}\vec{e_i}, \frac{2u}{1+u^2}\vec{e_j}, 0\right). \tag{A.1}$$

Definition A.1.1. *An arc $\mathcal{A}$ of a circle is given by a plane, a center and a radius r of the circle containing the arc and the parameter values of two extremities of $\mathcal{A}$ with respect to their increasing values in $[0, 2\pi]$ according to the trigonometric parameterization*

$$(r\cos(u), r\sin(u), 0) \tag{A.2}$$

of the unit circle centered at $\mathcal{O}$ and of radius r in the XY-plane. The direction of the arc is decided weather a randomly chosen third point on the circle belongs to the arc.

Notation A.1.3. *A line L in $\mathbb{R}^3$ is given by a point $P_0 = (x_0, y_0, z_0)$ and a non-zero vector $\vec{V} = \begin{pmatrix} a \\ b \\ c \end{pmatrix}$ in space such that L can be parameterized by $t \mapsto P_0 + t\vec{V}$ where t is a parameter in $\mathbb{R}$.*

Definition A.1.2. *The distance between any two points $p_1 = (x_1, y_1, z_1)$ and $p_2 = (x_2, y_2, z_2)$ in $\mathbb{R}^3$ is defined as*

$$\text{dist}(p_1, p_2) = ||p_1 - p_2||_2 = \sqrt{(x_1-x_2)^2 + (y_1-y_2)^2 + (z_1-z_2)^2}.$$

Definition A.1.3. *With the previous notation, distance function between $\mathcal{C}$ and L is defined as*

$$\text{dist}(\mathcal{C}(u), L(t)) = \sqrt{(\frac{1-u^2}{1+u^2} - (x_0+ta))^2 + (\frac{2u}{1+u^2} - (y_0+tb))^2}.$$

The critical points on $\mathcal{C}$ and on L are defined to be the couples of points (p_c, p_l) which are the critical points of the partial derivatives P_1 and P_2 of the square distance function between $\mathcal{C}$ and L such that

$$P_1 = (L(t) - \mathcal{C}(u))(\frac{d\mathcal{C}}{du}) \text{ and } P_2 = (L(t) - \mathcal{C}(u))(\frac{dL}{dt}).$$

Then, the distance between $\mathcal{C}$ *and* L *is*

$$\operatorname{dist}(\mathcal{C}, L) = \min_{(u,t)\in\mathbb{R}^2} \{\operatorname{dist}(\mathcal{C}(u), L(t))\}.$$

The closest points on $\mathcal{C}$ *and on* L*, are defined to be couples of critical points* (p_c, p_l) *minimizing the distance function between the circle* $\mathcal{C}$ *and the line* L*, i.e.*

$$\{(p_c, p_l) : p_c \in \mathcal{C}\ p_l \in L \text{ and } \operatorname{dist}(p_c, p_l) = \operatorname{dist}(\mathcal{C}, L)\}.$$

A.2 Overview of existing methods in TopSolid software computing the distance between an arc of a circle and a line in space

In this section, we explain the existing algorithms in TopSolid's library. They have two algorithms for computing couples of closest points on an arc of a circle and a line : the first one computes on the parameter value of circle, the second one computes on the parameter value of the line.

A.2.1 On parameter value of circle

This approach also uses elementary geometry and a solver computing solutions of a degree four polynomial equation. Firstly, it picks randomly a point P on the circle $\mathcal{C}$, and it projects orthogonally this point and the center of $\mathcal{C}$ onto L. Denote them as M and A respectively. After that, it considers the critical points of the polynomial obtained by Pythagore Theorem in the triangle $\widehat{PMA}$ as the candidates of the parameter values of the closest points p_c on $\mathcal{C}$.

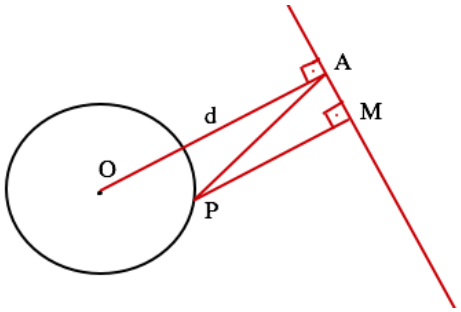


FIGURE A.1: Illustration of the $\widehat{PMA}$ from which TopSolid computes the critical points (p_c, p_l).

A.2.2 On parameter value of line

We explain the existing algorithm in TopSolid which computes the distance using the parameter value of the given line. Similarly to §A.2.1, this approach also uses elementary geometry and a solver for computing the solutions of a degree four polynomial equation. Firstly, it projects the line L into the plane of the circle $\mathcal{C}$. After that, it picks randomly a point P on L, and projects it orthogonally on $\mathcal{C}$, denotes this point as M and on XY-plane, denotes this point as P' . Finally, it studies the critical points of the polynomial obtained by using Pythagore Theorem in the triangle $\widehat{PP'M}$ as parameter value of the candidates of the closest points on the line L.

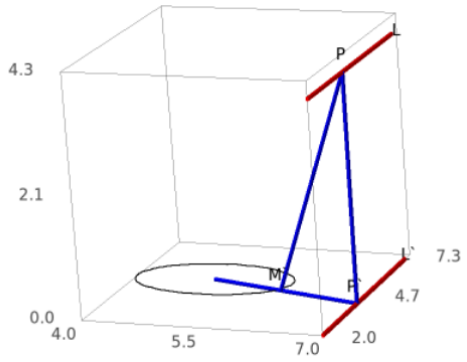


FIGURE A.2: Illustration of the $\widehat{PP'M}$ from which TopSolid computes the critical points (p_c, p_l).

A.3 Problem 1 : Distance between a circle and a line in space

In this section, how we treated the distance problem between a circle and a line in space is explained. The new algorithm mainly considers the resultant of two partial derivatives of the square distance function between the circle and the line (resultant of P_1 and P_2 given in (A.8)) depending on the parameter value of the line. The choice of eliminating the parameter value of the circle is based on the fact that the rational parameterization of the unit circle in XY-plane given in (A.1) causes distorsion around the point $(-1, 0, 0) \in \mathbb{R}^3$. The closer the critical point is to $(-1, 0, 0)$, the more we have numerical unstability. This is because the limit of the derivative of the coordinates of the parameterization approaches fast to zero, while the parameter value of the parameterization is going to $-\infty$. Solutions of resultant that we consider are computed by using a TopSolid's solver based on Ferrari's solutions for quartics. The case of the line is perpendicular to the plane where the circle is and the case of the line and the circle are both in the same plane are simplier and they do not require the resultant computation. In order to reduce the computation time, we studied such a distance problem in three cases.

In the sequel, the circle $\mathcal{C}$ and the line L are as in Notation A.1.2 and Notation A.1.3, respectively. We recall that

$$L(t) = \begin{pmatrix} x_0 \\ y_0 \\ z_0 \end{pmatrix} + \begin{pmatrix} a \\ b \\ c \end{pmatrix} t,$$

where t is a real parameter value. Assume that $\mathcal{C}$ and L do not intersect. We may always apply an affine transformation to the circle $\mathcal{C}$ and the line L which sends the circle to XY-plane and its center to the origin. We always consider $\mathcal{C}$ and L multiplied by such a matrix and denote them as $\mathcal{C}'$ and L', respectively. We call this multiplication as *preparation step* for our algorithms in this section. Similarly, one can multiply $\mathcal{C}'$ and L' and the couple of critical points (p'_c, p'_l) with the inverse of this transformation matrix to take them back into their initial positions. In this section, we call this inverse multiplication as *final step* in our algorithms. We recall that our algorithms exclude the case intersection of the circle and the line.

A.3.1 The line is perpendicular to the plane where the circle is located

In this case, with the previous notation we have $a = 0$ and $b = 0$. Also we have already mentioned that the new algorithm is based on the resultant computation. In §A.3.3, we will see that this resultant yields a polynomial of degree four. However, in this situation, there is only one couple of closest points (p_c, p_l) on the circle $\mathcal{C}$ and the line L, which is proved later in Proposition A.3.1. In addition, if line is perpendicular to the plane of circle and passing through its center, we have infinite number of critical points. This case is detected and the algorithm deals with the case where there is a finite number of critical points.

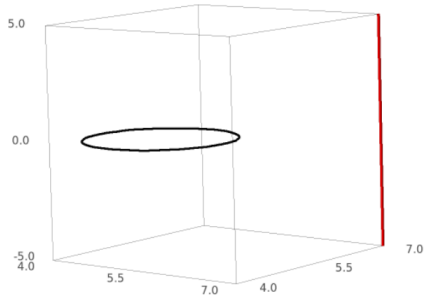


FIGURE A.3: The circle is in XY-plane, and the line is vertically passing through the XY-plane.

Lemma A.3.1. *The critical points p_l and p_c on L and $\mathcal{C}$ respectively are the couple of points (p_c, p_l) such that p_l is the point where L intersects with XY-plane, i.e. $p_l = (x_0, y_0, 0)$ for $x, y \in \mathbb{R}$ and*

$$p_c = (\frac{x_0 r}{||p_l||}, \frac{y_0 r}{||p_l||}, 0), \tag{A.3}$$

where $||p_l|| \neq 0$ and $||.||$ stands for the Euclidean norm.

Lemma A.3.2. *The distance between $\mathcal{C}$ and L is*

$$\text{dist}(\mathcal{C}, L) = \text{dist}(\mathcal{C}, p_l) = |\sqrt{x_0^2 + y_0^2} - r|. \tag{A.4}$$

Here the case $||p_l|| = 0$ is detected by the algorithm and it is excluded, since it is the case of infinite number of critical points.

A.3.2 The line is in the same plane as the circle

In this case, with the previous notation, we have $z_0 = 0$ and $c = 0$.

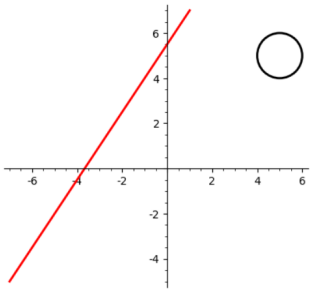


FIGURE A.4: The circle and the line are both in XY-plane.

Lemma A.3.3. *The critical points p_c and p_l on $\mathcal{C}$ and L respectively are the couple of points (p_c, p_l) such that p_l is closest point of L to the origin and*

$$p_c = (\frac{x_0 r}{||p_l||}, \frac{y_0 r}{||p_l||}, 0), \tag{A.5}$$

where $||p_l|| \neq 0$ and $||.||$ stands for the Euclidean norm. Thus, p_l can be computed by the extremas of the square distance function between L and the origin $\mathcal{O}$, i.e p_l is obtained for t value satisfying

$$(L(t) - \mathcal{O})\frac{dL(t)}{dt} = 0 \Leftrightarrow t = \frac{-(ax_0 + by_0)}{a^2 + b^2}. \tag{A.6}$$

Remark A.3.1. *One may notice that $a^2 + b^2$ is never equal to 0 because it is only the case where L is perpendicular to the plane of circle, i.e. §A.3.1.*

Lemma A.3.4. *Let $p_l = (x_l, y_l, 0)$. Then, the distance between $\mathcal{C}$ and L is given by the distance function*

$$\text{dist}(\mathcal{C}, L) = \sqrt{x_l^2 + y_l^2} - r. \tag{A.7}$$

A.3.3 General case

In order to find the distance between the circle $\mathcal{C}$ and the line L, one may look for the parameter values either t or u which minimize the distance function between L and $\mathcal{C}$

$$dist(L(t), C(u)).$$

For this reason, we study the square distance function between L and $\mathcal{C}$, i.e.

$$||L(t) - C(u)||^2,$$

and its extremas, i.e.

$$P_1 = (L(t) - \mathcal{C}(u))(\frac{d\mathcal{C}}{du}) = 0 \text{ and } P_2 = (L(t) - \mathcal{C}(u))(\frac{dL}{dt}) = 0. \tag{A.8}$$

We denote the resultant of P_1 and P_2 with respect to parameter u by $\text{Res}_u(P_1, P_2)$. $\text{Res}_u(P_1, P_2)$ is a polynomial of degree 4 in t variable. Let t_1, t_2, t_3, t_4 be its roots. Then,

Lemma A.3.5. *Let $t_j \in \{t_1, t_2, t_3, t_4\}$. The distance between $\mathcal{C}$ and L is given by*

$$\text{dist}(L, \mathcal{C}) = \min_{1 \leqslant j \leqslant 4} \{\text{dist}(L(t_j), \mathcal{C}) = \sqrt{(\sqrt{(x_0 + at_j)^2 + (y_0 + bt_j)^2} - r)^2 + (z_0 + xt_j)^2}\}. \tag{A.9}$$

Lemma A.3.6. *The closest points p_c and p_l on $\mathcal{C}$ and L respectively are the couples of points (p_c, p_l) such that*

$$p_c = (\frac{(x_0 + at_i)r}{||p_l||}, \frac{(y_0 + bt_i)r}{||p_l||}, \frac{(z_0 + ct_i)r}{||p_l||}) \text{ and} \tag{A.10}$$

$$p_l = (x_0 + at_i, y_0 + bt_i, z_0 + ct_i) \tag{A.11}$$

for all t_i verifying the equation (A.9).

Notation A.3.1. *Let (p_{c_i}, p_{l_i}) for $i = 1, 2, 3, 4$ denote the critical points on the circle $\mathcal{C}$ and on the line L respectively.*

A.3.4 Some observations on the number of the real solutions of resultant in §A.3.3

In this section, using mainly root classification (see [84, 1]) of the resultant given in §A.3.3, we deduce the number of real solutions which are the critical point(s) for the distance function between the line and the circle given in Definition A.1.2.

Theorem A.3.1 ([84])**.** *Root classification for a quartic polynomial,*

$$a_0t^4 + a_1t^3 + a_2t^2 + a_3t + a_4, \quad (a_0 \neq 0),$$

gives the number of the real roots with multiplicities and the number of the complex roots.

1)	$D_4 > 0$	$\wedge$	$D_3 > 0$	$\wedge$	$D_2 > 0$				4 *real roots*
2)	$D_4 > 0$	$\wedge$	$(D_3 \leqslant 0$	$\vee$	$D_2 \leqslant 0)$				*no real root*
3)	$D_4 < 0$								2 *distinct real roots*
4)	$D_4 = 0$	$\wedge$	$D_3 > 0$						1 *double*, 2 *distinct real roots*
5)	$D_4 = 0$	$\wedge$	$D_3 < 0$						1*double real root*
6)	$D_4 = 0$	$\wedge$	$D_3 = 0$	$\wedge$	$D_2 > 0$	$\wedge$	$E = 0$		4 *real roots*
7)	$D_4 = 0$	$\wedge$	$D_3 = 0$	$\wedge$	$D_2 > 0$	$\wedge$	$E \neq 0$		1 *real root of multiplicity* 3 *and* 1 *distinct real root*
8)	$D_4 = 0$	$\wedge$	$D_3 = 0$	$\wedge$	$D_2 < 0$				*no real root*
9)	$D_4 = 0$	$\wedge$	$D_3 = 0$	$\wedge$	$D_2 = 0$				1 *real root of multiplicity* 4,

where

$$\begin{aligned}
D_2 &= 3a_1^2 - 8a_2a_0,\\
D_3 &= 16a_0^2a_4a_2 - 18a_0^2a_3^2 - 4a_0a_2^3 + 14a_0a_3a_1a_2 - 6a_0a_4a_1^2 + a_2^2a_1^2 - 3a_3a_1^3,\\
D_4 &= 256a_0^3a_4^3 - 27a_0^2a_3^4 - 192a_0^2a_3a_4^2a_1 - 27a_1^4a_4^2 - 6a_0a_1^2a_4a_3^2 + a_2^2a_3^2a_1^2 - 4a_0a_2^3a_3^2 +\\
&\quad 18a_2a_4a_1^3a_3 + 144a_0a_2a_4^2a_1^2 - 80a_0a_2^2a_4a_1a_3 + 18a_0a_2a_3^3a_1 - 4a_2^3a_4a_1^2 - 4a_1^3a_3^3 +\\
&\quad 16a_0a_2^4a_4 - 128a_0^2a_2^2a_4^2 + 144a_0^2a_2a_4a_3^2,\\
E &= 8a_0^2a_3 + a_1^3 - 4a_0a_1a_2.
\end{aligned}$$

Proposition A.3.1. *The resultant of P_1 and P_2 (as in (A.8)) with respect to u, evaluated at $a = 0$ and $b = 0$, i.e. one considers the lines which are perpendicular to the plane of the circle with the notation of §A.3.1, has one real root of multiplicity 4. (The case of the line passing through the center of the circle for which there exist infinitely many closest points on the circle is excluded.)*

Proof. If $a = 0$ and $b = 0$, then by Theorem A.3.1 D_2, D_3 and D_4 become zero for all $c, x, y, z \in \mathbb{R}$. Hence, by the root classification above there exist one real root of multiplicity 4. □

Algorithm 3: Distance between the circle $\mathcal{C}$ and the line L.

Input : Circle $\mathcal{C}$, the line L as in Notation A.1.2 and Notation A.1.3 respectively.

Output: $\text{dist}(\mathcal{C}, L)$ and (p_{c_i}, p_{l_i}) for $i = 1, 2, 3, 4$.

1: Do the *preparation step*. Multiply $\mathcal{C}$ by a transformation matrix to send it to XY-plane and its center to the origin. Multiply L by the same matrix. Denote them as $\mathcal{C}'$ L' such that

$$L'(t) = \begin{bmatrix} x'_0 \\ y'_0 \\ z'_0 \end{bmatrix} + \begin{bmatrix} a' \\ b' \\ c' \end{bmatrix} t.$$

2: **if** (according to §A.3.1) $L' \perp XY$*-plane* **then**

Compute the point $(x'_0, y'_0, 0)$ and denote it as p'_{l_1}.

Compute the point $(\frac{x'_0 r}{||p'_l||}, \frac{y'_0 r}{||p'_l||}, 0)$ and denote it as p'_{c_1}.

Do the *final step* i.e. multiply p'_{l_1}, p'_{c_1} by the inverse of the transformation matrix in Step 1. Denote them as p_{l_1}, p_{c_1}.

Compute the distance $\text{dist}(p_l, \mathcal{C}) = |\sqrt{x'^2_0 + y'^2_0} - r|$.

3: **else if** (according to §A.3.2) $L' \subset XY$*-plane* **then**

Compute the point $\frac{-(a'x'_0 + b'y'_0)}{a'^2 + b'^2}$ and denote it as t.

Compute $p + \vec{V}t$ and denote it as p'_{l_1}.

Compute the point $(\frac{x'_0 r}{||p'_{l_1}||}, \frac{y'_0 r}{||p'_{l_1}||}, 0)$ and denote it as p'_{c_1}.

Compute the point $(x_l, y_l, 0)$ and denote it as p'_{l_1}.

Do the *final step* i.e. multiply p'_{l_1}, p'_{c_1} by the inverse of the transformation matrix in Step 1. Denote them as p_{l_1}, p_{c_1}.

Compute the distance $\text{dist}(\mathcal{C}, L) = \sqrt{x_l^2 + y_l^2} - r$.

4: **else**

(according to §A.3.3)

(a) Evaluate the closed form of the resultant in §A.3.3 and solve it. Denote its solutions as t_1, t_2, t_3, t_4.

(b) Go to the algorithm (based on the Theorem A.3.1 to get the number of the real solutions of the resultant in the previous step. Denote it as k.

for $i = 1$ *to* k **do**

Compute the point $p + \vec{v}t'_i$ and denote it as p'_{l_i}.

Compute the point $(\frac{(x'_0 + a't'_i)r}{||p'_{l_i}||}, \frac{(y_0 + b't'_i)r}{||p'_{l_i}||}, \frac{(z_0 + c't'_i)r}{||p'_{l_i}||})$ and denote it as p'_{c_i}.

Compute the distance $d_i := \text{dist}(p'_{l_i}, p'_{c_i}) = \sqrt{|\sqrt{(x'_0 + a't'_i)^2 + (y'_0 + b't'_i)^2} - r|^2 + (z'_0 + c't'_i)^2}$

Store all d_i's.

Denote $\min(d_1, d_2, d_3, d_4)$ as $\text{dist}(\mathcal{C}, L)$.

Do the *final step* i.e. multiply p'_{l_1}, p'_{c_1} by the inverse of the transformation matrix in Step 1. Denote them as p_{l_1}, p_{c_1}.

A.4 Problem 2 : Distance between an arc of a circle and a line segment in space

The new Algorithm for distance between an arc of a circle and a line segment uses the outputs of the Algorithm 3 for problem 1, described in §A.3, on which we apply the preparation step. Namely its inputs are the outputs of the Algorithm 3 multiplied by a transformation matrix which sends the circle $\mathcal{C}$ to the XY-plane and its center to the origin. Let $\mathcal{C}', L', p'_l, p'_c$ be respectively the transformed $\mathcal{C}, L, p_l, p_c$ by a such transformation matrix.

Notation A.4.1. *Let e_{a_1}, e_{a_2} denote the extremities of the arc $\mathcal{A}$ of $\mathcal{C}$ with respect to the direction of the arc $\mathcal{A}$ as in Definition A.1.1.*

Definition A.4.1. *A segment S of the line L is parameterized as $S(t) = (1-t)s_1+ts_2$ with $t \in [0,1]$ where e_{s_1}, e_{s_2} are its extremities.*

For the case that line is perpendicular to the circle plane, described in §A.3.1, and they are both in the same plane, described in §A.3.2, the Algorithm 3 finds one couple of closest points (p_c, p_l). For the general case §A.3.3, the algorithm runs for each couple (p_c, p_l) obtained by the real roots of the resultant of the equations giving extremas of the square distance function between the circle and the line, described in §A.3.3.

The algorithm considers the distance computation into 2 cases : the closest points (p_l, p_c) on L and on $\mathcal{C}$ are contained simultaneously in S and $\mathcal{A}$ respectively and the other situations.

Notation A.4.2. *Let the orthogonal projections of the extremities of the line segment onto the circle be denoted by $e_{s_1}^{proj}, e_{s_2}^{proj}$ also the orthogonal projections of the extremities of the arc onto the line be denoted by $e_{a_1}^{proj}, e_{a_2}^{proj}$.*

Let's recall how we compute the orthogonal projection of a point $p = (x_0, y_0, z_0) \in \mathbb{R}^3$ on to the given circle in XY-plane. We denote it by p^{proj}. We project orthogonally the point on XY-plane, denote it by p_{XY}. Hence, $p_{XY} = (x_0, y_0, 0)$, then do dilation and we have $p^{proj} = (\frac{rx_0}{||p^{proj}||}, \frac{ry_0}{||p^{proj}||}, 0)$.

Mainly, the algorithm considers the extremities of the line segment and the arc, the orthogonal projections of the extremities of the line segment onto circle which belong to the arc, $e_{s_1}^{proj}, e_{s_2}^{proj}$, the orthogonal projections of the extremities of the arc onto the line which belong to the line segment, $e_{a_1}^{proj}, e_{a_2}^{proj}$ and the couple closest points of the circle and the line as the candidates to be the couple of closest points of the arc and the line segment.

A.4.1 If p_l and p_c are both contained in $\mathcal{S}$ and $\mathcal{A}$ respectively where (p_l, p_c) is a couple of closest points of L and $\mathcal{C}$

This case is trivial.

Lemma A.4.1. *The couples of closest points (p_s, p_a) on segment S of L and the arc $\mathcal{A}$ of $\mathcal{C}$ are the couples of closest points (p_l, p_c) on the line L and on the circle $\mathcal{C}$.*

A.4.2 If either p_l or p_c is not contained in $\mathcal{S}$ and $\mathcal{A}$ respectively where (p_l, p_c) is a couple of closest points of L and $\mathcal{C}$

Let's start by looking for some critical points different than the solutions of the resultant described in §A.3.3.

Notation A.4.3. *Let $e_{s_i}^{pp}$ denotes the orthogonal projection of $e_{s_i}^{proj}$ onto L for $i = 1, 2$.*

Proposition A.4.1. *Let $p^{proj} = (\frac{x_0 r}{\sqrt{x_0^2+y_0^2}}, \frac{y_0 r}{\sqrt{x_0^2+y_0^2}}, 0)$ be the orthogonal projection of a point $p = (x_0, y_0, z_0)$ of L onto $\mathcal{C}$ in XY-plane, centered at origin. Since the orthogonal projection p^{pp} of p^{proj} onto L is not necessarily p in general for any p, then neither for e_{s_i} where $i = 1, 2$. Moreover, two distances*

$$\{dist(e_{s_1}^{proj}, e_{s_1}^{pp}), dist(e_{s_2}^{proj}, e_{s_2}^{pp})\}$$

are also candidates to be $\mathrm{dist}(\mathcal{A}, L)$ *(see Figure A.5).*

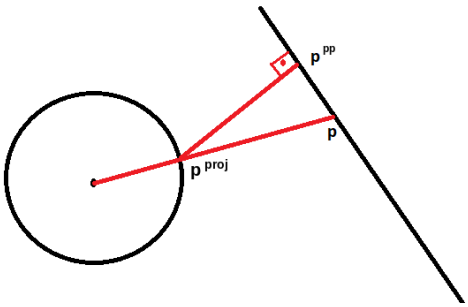


FIGURE A.5: The point p having orthogonal projection p^{proj} on the circle which is different than the orthogonal projection of p^{proj} onto the line, denoted by p^{pp}.

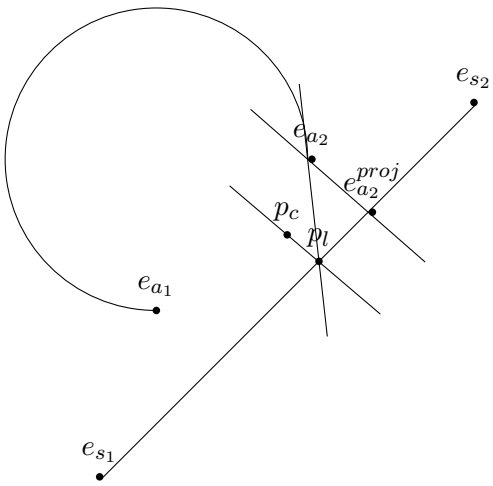


FIGURE A.6: If the arc and the circle are in the plane and closest point p_c of circle is not contained on the arc, then the orthogonal projection of e_{a_2} onto L, denoted by $e_{a_2}^{proj}$ gives smaller distance to S.

Proposition A.4.2. *For the case p_l is contained in S and the p_c is not contained in $\mathcal{A}$, for all $i = 1, 2$,*

$$\mathrm{dist}(e_{a_i}^{proj}, e_{a_i}) < \mathrm{dist}(e_{a_i}, p_l).$$

Proof. By Pythagore in the triangle $(p_l, e_{a_i}^{proj}, e_{a_i})$,

$$\mathrm{dist}(e_{a_i}, p_l)^2 = \mathrm{dist}(e_{a_i}^{proj}, e_{a_i})^2 + \mathrm{dist}(e_{a_i}^{proj}, p_l)^2.$$

The equality is obtained only for $e_{a_i}^{proj} = p_c$, which is not possible by assumption. □

Lemma A.4.2. *The distance between $\mathcal{A}$ and S is*

$$\begin{aligned}\mathrm{dist}(\mathcal{A}, S) = \quad & \min\{\mathrm{dist}(e_{s_1}^{proj}, e_{s_1}), \mathrm{dist}(e_{s_2}^{proj}, e_{s_2}), \mathrm{dist}(e_{a_1}, e_{s_1}), \mathrm{dist}(e_{a_1}, e_{s_2}),\\ & \mathrm{dist}(e_{a_1}, e_{a_1}^{proj}), \mathrm{dist}(e_{a_2}, e_{a_2}^{proj}), \mathrm{dist}(e_{a_2}, e_{s_1}), \mathrm{dist}(e_{a_2}, e_{s_2}),\\ & \mathrm{dist}(e_{s_1}^{proj}, e_{s_1}^{pp}), \mathrm{dist}(e_{s_2}^{proj}, e_{s_2}^{pp})\}.\end{aligned}$$

Lemma A.4.3. *The couples of closest points (p_s, p_a) on segment S of L and on the arc $\mathcal{A}$ of $\mathcal{C}$ are the couples of points which are considered in Lemma A.4.2 and whose distance in between is equal to the* $\mathrm{dist}(\mathcal{A}, S)$.

Algorithm 4: Distance between the arc $\mathcal{A}$ of the circle $\mathcal{C}$ and the line segment S.

Input : $\mathcal{A}$ and S are given as in Definition A.1.1 and Definition A.4.1 respectively and (p_c, p_l) couple of closest points of $\mathcal{C}$ and of L, $\mathrm{dist}(p_c, p_l)$.

Output: $\mathrm{dist}(\mathcal{A}, S)$ and (p_{a_i}, p_{s_i}), for $1 \leqslant i \leqslant 2$.

1: Do the *preparation step*. Multiply $\mathcal{C}$ by a transformation matrix to send it to XY-plane and its center to the origin, denote it by $\mathcal{C}'$. Multiply L, p_c, p_l by the same matrix and denote them by L', p_c', p_l'.

2: **if** (according to §A.4.1) $p_l' \subset S$ *and* $p_c' \subset \mathcal{A}$ **then**

Denote $p_{a_1}' := p_c'$;
Denote $p_{s_1}' := p_l'$;
Denote $\mathrm{dist}(\mathcal{A}, S) := \mathrm{dist}(p_c', p_l')$;
Do the *final step*, i.e. multiply p_{a_1}', p_{s_1}' by the inverse of the transformation matrix in Step 1. Denote them as p_{a_1}, p_{s_1};

3: **else**

(according to §A.4.2);

(a) Compute the $\min\{\mathrm{dist}(e_{s_1}^{proj}, e_{s_1}), \mathrm{dist}(e_{s_2}^{proj}, e_{s_2}), \mathrm{dist}(e_{a_1}, e_{s_1}), \mathrm{dist}(e_{a_1}, e_{s_2}), \mathrm{dist}(e_{a_1}, e_{a_1}^{proj}), \mathrm{dist}(e_{a_2}, e_{a_2}^{proj}), \mathrm{dist}(e_{a_2}, e_{s_1}), \mathrm{dist}(e_{a_2}, e_{s_2}), \mathrm{dist}(e_{s_1}^{proj}, e_{s_1}^{pp}), \mathrm{dist}(e_{s_2}^{proj}, e_{s_2}^{pp})\}$ and denote it as d.

(b) Let n be the number of the couples of points (a', b') in the previous Step satisfying $\mathrm{dist}(a', b') = d$.

(c) Denote $\mathrm{dist}(\mathcal{A}, S) = d$.

for $1 < i \leqslant n$ **do**

Denote $p_{a_i}' := a'$;
Denote $p_{s_i}' := b'$;
Do the *final step*, i.e. multiply p_{a_i}', p_{s_i}' by the inverse of the transformation matrix in Step 1 for all $1 < i \leqslant n$. Denote them as p_{a_i}, p_{s_i};

A.5 Observations

1. It was difficult to separate the cases using conditions on the point and the vector defining the line L as in Notation A.1.3, more precisely on a, b, c, z values, because of the tolerance choice. I could manage to separate them better with a condition based on angles. I considered 10^{-5} as linear tolerance, and 0.000872664625997165 as angular tolerance.

2. I had to decrease the use of square root function, because it was changing the result numerically.

3. I chose to eliminate the variable of the line instead of the circle from the resultant of two partial derivatives of square distance function between the circle and the line (see §A.3.3), because the rational parameterization of the circle given in Notation A.1.2 causes numerical instability around the point $(-1, 0, 0)$. Otherwise, it was necessary to detect whether the critical points of the circle were closed enough to the point $(-1, 0, 0)$. In this case, we would consider also the parameterization of the circle obtained by exchanging the x and y coordinates of the rational parameterization of unit circle in XY-plane given in Notation A.1.2.

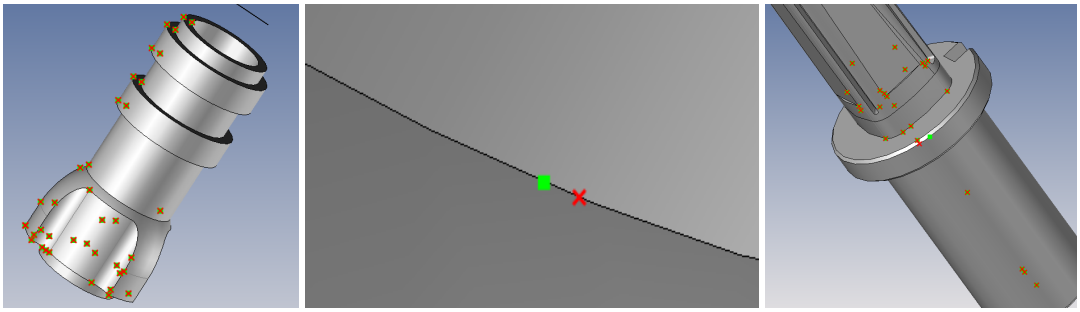
4. Problem 1 looks for the real solutions of resultant given in §A.3.3. It was difficult to fix a tolerance from which the imaginary part of the solutions are small enough to see them as reals. For this reason, I implemented Proposition A.3.1, to separate the number of the real solutions for a quartic polynomial equation.

A.6 Problems of existing algorithms

(a) Existing methods do not consider all the critical points of the corresponding distance function.

(b) Existing methods do not consider the line segments. They consider only the entire lines.

(c) One problem was two existing algorithms described in §A.2 find different closest points on the circle. The following 3 pictures are done on a sketch designed by a client. For this sketch, I had made run the debugging code. The green and red points are the closest points on the circles to the choosen line by mouse (the line which is perpendicular to the screen passing through the mouse) respectively computed by the 1st (using the parameter of the circle) and the 2nd existing algorithm (using the parameter of the line) in TopSolid. One may see that two algorithms may find different closest points.



The existing methods were failing also because segments were seen as lines and not all the critical points coming from the resultant in A.3.3 were considered. Moreover, it was also coming from numerical instability of considering parameter value of circle as explained in §A.5.

A.7 Comparison and validation

(a)

Example A.7.1. *Let's consider the arc of a circle of center* $(-0.0266955245595897, 0.0003048, -0.0277528286830878)$*, of radius* 0.0003048*, for the parameter values according to the trigonometric parametrization of the circle is in the interval* $[4.71238898038469, 6.28318530717957]$ *and the line given by the point* $(0.0248195074144692, 0.164721630786812, 0.103374481857372)$*, and the unit vector* $(0.792993412407533, 0.392932291880139, -0.465580993894809)$*. The parameter value of the circle at the closest point* p_a *is :*

Algorithm	*t value*
Existing	6.28318530717957
Algorithm 4	4.71238898038469

The coordinates of the closest point on the arc are:

Algorithm	p_s
Existing	$(-0.0268353856911874, 0.000304799999999994, -0.0280236457871787)$
Algorithm 4	$(-0.0266955245595897, 0, -0.0277528286830878)$

Distance between the closest point on the line computed via the existing algorithm on the parameter value of line and via Algorithm 4 is 0.000431052293811291.

(b) One may use the interface and use distance icon to experiment only one distance computation for each click. In that case one may always find that orthogonality verification, which is whether the closest point of the line is a orthogonal projection of the closest point on the circle, is always satisfied for the first case §A.4.1 of the Algorithm 4.

There exist a debugging code which computes, according to both existing methods, the closest points on the all circles in the document to the chosen axis by the mouse which is perpendicular to the screen. By this debugging code, it is possible to compare several computations with one click. I converted it to comaparison of 4 methods: both existing methods, my Algorithm 4, and the solutions of ParaSolid which is an external module of TopSolid. My experiments show that the Algorithm 4 coincide with the solutions as ParaSolid.

(c) Following two examples of the case §A.4.1, i.e. the closest points of the circle are on the arc and the closest point of the line are on the segment show that the Algorithm 4 approches more to the closest points than the existing algorithms.

Example A.7.2. *Let's consider the circle of center* $(4.36210433058997, -0.614943620347628, 0)$*, of radius* 0.369226219157435*, and the line given by the point* $(4.95987269404932, 2.1814917423629, -2.95370611561499)$*, and the unit vector* $(0.881513709084022, -0.216813525604839, 0.419434709831851)$*. The parameter value of the circle at the closest point is :*

Algorithm	t
Existing	0.923216306958422
Algorithm 4	0.923400665174119

The coordinates of the closest point on the circle are:

Algorithm	p_s
Existing	$(4.58484304856623, -0.320468724257, 0)$
Algorithm 4	$(4.58478875591491, -0.320427665548919, 0)$

Distance between the closest point on the line computed via the existing algorithm on the parameter value of line and via Algorithm 4 is $6.80698868559901E-05$.
The computation time for both methods are as following:

Algorithm	*time*
Existing	00 : 00 : 00.0001944
Algorithm 4	00 : 00 : 00.0000645

Example A.7.3. *Let's consider the circle of center* $(-1.72615113008238, 1.74841631272117, 1.61159839442974)$*, of radius* 0.5*, and the line given by the point* $(4.78198822485689, 1.8633299601087, -2.74431519387126)$*, and the unit vector* $(0, 881513709084022, -0, 216813525604839, 0, 419434709831851)$.
The parameter value of the circle at the closest point p_c *is :*

Algorithm	t
Existing	5.62854848049478
Algorithm 4	5.62833550554993

The coordinates of the closest point on the circle are:

Algorithm	p_s
Existing	$(-1.33903540200799, 1.48554519129016, 1.43541614051341)$
Algorithm 4	$(-1.33910276791265, 1.48547876876287, 1.43536725836432)$

Distance between the closest point on the line computed via the existing algorithm on the parameter value of line and via Algorithm 4 is 0.000106487472223496.
The computation time for both methods are as following:

Algorithm	*time*
Existing	00 : 00 : 00.0000966
Algorithm 4	00 : 00 : 00.0000647

(d) I did Newton iterations on 677 examples of the case in A.4.1, having different closest points then the Algorithm 3 finds. They all converged to the closest points on the circle computed by the Algorithm 3.

(e) The average computation time is (over 457710 examples)

Algorithm	time
Existing	00 : 00 : 00.0000966
Algorithm 4	00 : 00 : 00.0000643

(f) 67842 among 457710, i.e, %14.82204, computations on the client's examples, have different solutions from the new Algorithm 4 with the tolerance 10^{-5}.

Bibliography

[1] Dennis S. Arnon. "Geometric reasoning with logic and algebra". In: *Artificial Intelligence* 37.1 (1988), pp. 37 –60. ISSN: 0004-3702. DOI: https://doi.org/10.1016/0004-3702(88)90049-5. URL: http://www.sciencedirect.com/science/article/pii/0004370288900495.

[2] N. Botbol, L. Busé, and M. Chardin. "Fitting ideals and multiple points of surface parameterizations". In: *Journal of Algebra* 420 (2014), pp. 486–508. ISSN: 0021-8693. DOI: http://dx.doi.org/10.1016/j.jalgebra.2014.07.028. URL: http://www.sciencedirect.com/science/article/pii/S0021869314004463.

[3] N. Botbol and A. Dickenstein. "Implicitization of rational hypersurfaces via linear syzygies: A practical overview". In: *Journal of Symbolic Computation* 26.74 (2016), pp. 493–512. DOI: 10.1016/j.jsc.2015.09.001.

[4] N. Botbol, A. Dickenstein, and M. Dohm. "Matrix representations for toric parametrizations". In: *Computuer Aided Geometric Design* 26.7 (2009), pp. 757–771. ISSN: 0167-8396. DOI: 10.1016/j.cagd.2009.03.005. URL: http://dx.doi.org/10.1016/j.cagd.2009.03.005.

[5] Nicolás Botbol. "The implicit equation of a multigraded hypersurface". In: *Journal of Algebra* 348.1 (2011), pp. 381–401. ISSN: 0021-8693. DOI: http://dx.doi.org/10.1016/j.jalgebra.2011.09.019. URL: http://www.sciencedirect.com/science/article/pii/S0021869311005369.

[6] Nicolás Botbol and Marc Chardin. "Castelnuovo Mumford Regularity with respect to multigraded ideals". In: *Journal of Algebra* 474 (July 2011). DOI: 10.1016/j.jalgebra.2016.11.017.

[7] N. Bourbaki. *Algèbre Chapitre X*. Masson S.A., 1980.

[8] M. P. Brodmann and R. Y. Sharp. *Local Cohomology: An Algebraic Introduction with Geometric Applications*. 2nd ed. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2012. DOI: 10.1017/CBO9781139044059.

[9] W. Bruns and H. J. Herzog. *Cohen-Macaulay Rings*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 1998. ISBN: 9780521566742. URL: https://books.google.fr/books?id=LF6CbQk9uScC.

[10] D. A. Buchsbaum and D. Eisenbud. "Remarks on ideals and resolutions". In: *Symposia Math. IV(Istituto Nazionali di Alta Matematica)* (1973), pp. 255–283.

[11] L. Busé and M. Chardin. "Implicitizing rational hypersurfaces using approximation complexes". In: *Journal of Symbolic Computation* 40.4-5 (2005), pp. 1150–1168. DOI: 10.1016/j.jsc.2004.04.005.

[12] L. Busé, D.A. Cox, and C. D'Andrea. "Implicitization of surfaces in $\mathbb{P}^3$ in the presence of base points". In: *Journal of Algebra and Its Applications* 2.2 (2003), pp. 189–214. ISSN: 0219-4988.

[13] L. Busé and M. Dohm. "Implicitization of bihomogeneous parametrizations of algebraic surfaces via linear syzygies". In: *ISSAC 2007*. New York: ACM, 2007, pp. 69–76.

[14] L. Busé and J.P. Jouanolou. "On the closed image of a rational map and the implicitization problem". In: *Journal of Algebra* 265.1 (2003), pp. 312–357. ISSN: 0021-8693.

[15] L. Busé, H. Khalil, and B. Mourrain. "Resultant-based methods for plane curves intersection problems". In: *Proceedings of the 8th International Conference on Computer Algebra in Scientific Computing*. CASC'05. Kalamata, Greece: Springer-Verlag, 2005, pp. 75–92. ISBN: 3-540-28966-6, 978-3-540-28966-1. DOI: 10.1007/11555964_7. URL: http://dx.doi.org/10.1007/11555964_7.

[16] L. Busé and T. Luu Ba. "Matrix-based implicit representations of rational algebraic curves and applications". In: *Computer Aided Geometric Design* 27.9 (2010), pp. 681–699. DOI: 10.1016/j.cagd.2010.09.006.

[17] L. Busé and T. Luu Ba. "The surface/surface intersection problem by means of matrix based representations". In: *Computer Aided Geometric Design* 29.8 (2012), pp. 579–598. DOI: 10.1016/j.cagd.2012.04.002. URL: https://hal.inria.fr/inria-00620947.

[18] Laurent Busé. "Implicit matrix representations of rational Bézier curves and surfaces". In: *Computer-Aided Design* 46 (2014). 2013 SIAM Conference on Geometric and Physical Modeling, pp. 14–24. ISSN: 0010-4485. DOI: http://dx.doi.org/10.1016/j.cad.2013.08.014. URL: http://www.sciencedirect.com/science/article/pii/S0010448513001541.

[19] Laurent Busé, Marc Chardin, and Aron Simis. "Elimination and nonlinear equations of Rees algebra". In: *Journal of Algebra* 324 (Nov. 2009), pp. 1314–1333. DOI: 10.1016/j.jalgebra.2010.07.006.

[20] Laurent Busé, Clément Laroche, and Fatmanur Yıldırım. "Implicitizing rational curves by the method of moving quadrics". In: *Computer-Aided Design* 114 (2019), pp. 101 –111. ISSN: 0010-4485. DOI: https://doi.org/10.1016/j.cad.2019.05.019. URL: http://www.sciencedirect.com/science/article/pii/S0010448519301927.

[21] J.W.S. Cassels, J.W.S. Cassels, C.M. Series, and J.W. Bruce. *Local Fields*. Cambridge Computer Science Texts. Cambridge University Press, 1986. ISBN: 9780521315258. URL: https://books.google.fr/books?id=UY52SQnV9w4C.

[22] M. Chardin, A.L. Fall, and U. Nagel. "Bounds for the Castelnuovo-Mumford regularity of modules". In: *Mathematische Zeitschrift 258(1)* 258.1 (2008), pp. 69–80. ISSN: 0025-5874. DOI: 10.1007/s00209-007-0157-9. URL: https://doi.org/10.1007/s00209-007-0157-9.

[23] Marc Chardin. "Implicitization using approximation complexes". In: *Algebraic geometry and geometric modeling*. Springer, 2006, pp. 23–35.

[24] Marc Chardin. "Regularity of ideals and their powers". In: (Oct. 2013).

[25] Marc Chardin, Steven Dale Cutkosky, and Quang Hoa Tran. "Fibers of rational maps and Jacobian matrices". In: *Journal of Algebra* (2019). ISSN: 0021-8693. DOI: https://doi.org/10.1016/j.jalgebra.2019.01.035. URL: http://www.sciencedirect.com/science/article/pii/S0021869319300894.

[26] F. Chen and W. Wang. "The μ-basis of a planar rational curve - properties and computation". In: *Graphical Models* 64 (Feb. 2003), pp. 368–381. DOI: 10.1016/S1077-3169(02)00017-5.

[27] Henri Cohen. *A course in computational algebraic number theory*. Berlin, Heidelberg: Springer-Verlag, 1993. ISBN: 0-387-55640-0.

[28] D. A. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra, 3/e (Undergraduate Texts in Mathematics)*. Berlin, Heidelberg: Springer-Verlag, 2007. ISBN: 0387356509.

[29] D.A. Cox, R. Goldman, and M. Zhang. "On the validity of implicitization by moving quadrics of rational surfaces with no base points". In: *J. Symbolic Comput.* 29.3 (2000), pp. 419–440. ISSN: 0747-7171. DOI: 10.1006/jsco.1999.0325.

[30] D.A Cox, J. Little, and D. O'Shea. *Using algebraic geometry*. Vol. 185. Graduate Texts in Mathematics. New York: Springer-Verlag, 1998. ISBN: 0-387-98487-9; 0-387-98492-5.

[31] D.A. Cox, T. W. Sederberg, and F. Chen. "The moving line ideal basis of planar rational curves". In: *Computer Aided Geometric Design* 15.8 (1998), pp. 803–827. ISSN: 0167-8396. DOI: http://dx.doi.org/10.1016/S0167-8396(98)00014-4. URL: http://www.sciencedirect.com/science/article/pii/S0167839698000144.

[32] David A. Cox. "Solving equations via algebras". In: *Solving polynomial equations*. Vol. 14. Algorithms Comput. Math. Springer, Berlin, 2005, pp. 63–123. DOI: 10.1007/3-540-27357-3_2. URL: https://doi.org/10.1007/3-540-27357-3_2.

[33] David A. Cox. "Bezoutians and Tate resolutions". In: *Journal of Algebra* 311.2 (2007), pp. 606–618. ISSN: 0021-8693. DOI: 10.1016/j.jalgebra.2006.11.029.

[34] Carlos D'Andrea. "On the structure of μ-classes". In: *Communications in Algebra - COMMUN ALGEBRA* 32 (Mar. 2004), pp. 159–165. DOI: 10.1081/AGB-120027858.

[35] G. M. Diaz-Toca and L. Gonzalez-Vega. "Barnett's theorems about the greatest common divisor of several univariate polynomials through Bézout-like matrices". In: *Journal of Symbolic Computation* 34.1 (2002), pp. 59–81. ISSN: 0747-7171. DOI: 10.1006/jsco.2002.0542.

[36] M. Dohm and S. Zube. "The implicit equation of a canal surface". In: *Journal of Symbolic Computation* 44.2 (2009), pp. 111 –130. ISSN: 0747-7171. DOI: https://doi.org/10.1016/j.jsc.2008.06.001. URL: http://www.sciencedirect.com/science/article/pii/S0747717108000916.

[37] A.V. Doria, S.H. Hassanzadeh, and A. Simis. "A characteristic-free criterion of birationality". In: *Advances in Mathematics* 230.1 (2012), pp. 390 –413. ISSN: 0001-8708. DOI: https://doi.org/10.1016/j.aim.2011.12.005. URL: http://www.sciencedirect.com/science/article/pii/S0001870811003999.

[38] J. Draisma, E. Horobeţ, G. Ottaviani, B. Sturmfels, and R.R Thomas. "The Euclidean distance degree of an algebraic variety". In: *Foundations of Computational Mathematics* (2015), pp. 1–51. ISSN: 1615-3383. DOI: 10.1007/s10208-014-9240-x. URL: http://dx.doi.org/10.1007/s10208-014-9240-x.

[39] P. Dreesen, K. Batselier, and B. De Moor. "Back to the roots: polynomial system solving, linear algebra, systems theory". In: *IFAC Proceedings Volumes* 45.16 (2012). 16th IFAC Symposium on System Identification, pp. 1203 –1208. ISSN: 1474-6670. DOI: https://doi.org/10.3182/20120711-3-BE-2027.00217. URL: http://www.sciencedirect.com/science/article/pii/S1474667015381179.

[40] J. A. Eagon and D. G. Northcott. "Ideals Defined by Matrices and a Certain Complex Associated with Them". In: *Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences* 269.1337 (1962), pp. 188–204. ISSN: 00804630. URL: http://www.jstor.org/stable/2992698.

[41] David Eisenbud. *Commutative algebra with a view toward algebraic geometry*. Vol. 150. Graduate Texts in Mathematics. New York: Springer-Verlag, 1995, pp. xvi+785. ISBN: 0-387-94268-8; 0-387-94269-6.

[42] David Eisenbud. *The Geometry of Syzygies*. Vol. 229. 0072-5285. Springer-Verlag New York, 2005. ISBN: 978-0-387-22215-8.

[43] W. Fulton. *Intersection theory*. Ergebnisse der Mathematik und ihrer Grenzgebiete. Springer-Verlag, 1984. ISBN: 9783540121763. URL: https://books.google.fr/books?id=cmoPAQAAMAAJ.

[44] Gene H. Golub and Charles F. Van Loan. *Matrix computations*. Third. Johns Hopkins Studies in the Mathematical Sciences. Baltimore, MD: Johns Hopkins University Press, 1996, pp. xxx+698. ISBN: 0-8018-5413-X; 0-8018-5414-8.

[45] F. Gouvea. *p-adic Numbers: An Introduction*. Universitext. Springer Berlin Heidelberg, 2003. ISBN: 9783540629115. URL: https://books.google.fr/books?id=g1QHBOBzo9kC.

[46] Joe Harris. *Algebraic geometry*. Vol. 133. Graduate Texts in Mathematics. A first course, Corrected reprint of the 1992 original. Springer-Verlag, New York, 1995. ISBN: 0-387-97716-3.

[47] Robin Hartshorne. *Algebraic geometry*. Graduate Texts in Mathematics, No. 52. Springer-Verlag, New York-Heidelberg, 1977. ISBN: 0-387-90244-9.

[48] J. Herzog, A. Simis, and W. V. Vasconcelos. "Approximation complexes of blowing-up rings, II". In: 1982.

[49] J. Herzog, A. Simis, and W. V. Vasconcelos. "Koszul homology and blowing-up rings". In: 1983.

[50] J Herzog, A Simis, and W.V Vasconcelos. "Approximation complexes of blowing-up rings". In: *Journal of Algebra* 74.2 (1982), pp. 466 –493. ISSN: 0021-8693. DOI: https://doi.org/10.1016/0021-8693(82)90034-5. URL: http://www.sciencedirect.com/science/article/pii/0021869382900345.

[51] H. Hong, Z. Hough, and Kogan I. "Algorithm for computing μ-bases of univariate polynomials". In: *Journal of Symbolic Computation* 80 (2017), pp. 844–874. ISSN: 0747-7171. DOI: 10.1016/j.jsc.2016.08.013.

[52] X. Jia, X. Shi, and F. Chen. "Survey on the theory and applications of μ-bases for rational curves and surfaces". In: *Journal of Computational and Applied Mathematics* 329 (2018). The International Conference on Information and Computational Science, 2–6 August 2016, Dalian, China, pp. 2–23. ISSN: 0377-0427. DOI: 10.1016/j.cam.2017.07.023.

[53] Xiaohong Jia, Haohao Wang, and Ron Goldman. "Set-theoretic generators of rational space curves". In: *Journal of Symbolic Computation* 45.4 (2010), pp. 414–433. ISSN: 0747-7171. DOI: 10.1016/j.jsc.2009.11.001. URL: http://dx.doi.org/10.1016/j.jsc.2009.11.001.

[54] A. Josse and F. Pene. "Normal class and normal lines of algebraic surfaces". Preprint arXiv:1402.7266. 2014.

[55] Jean-Pierre Jouanolou. "Formes d'inertie et résultant: un formulaire". In: *Advances in Mathematics* 126.2 (1997), pp. 119–250. ISSN: 0001-8708. DOI: 10.1006/aima.1996.1609.

[56] Jean-Pierre Jouanolou. "An explicit duality for quasi-homogeneous ideals". In: *Journal of Symbolic Computation* 44.7 (2009), pp. 864–871. ISSN: 0747-7171. DOI: 10.1016/j.jsc.2008.04.011. URL: https://doi.org/10.1016/j.jsc.2008.04.011.

[57] T. Krick, L.M. Pardo, and M. Sombra. "Sharp estimates for the arithmetic Nullstellensatz". In: *Duke Mathematical Journal* 109.3 (Sept. 2001), pp. 521–598. DOI: 10.1215/S0012-7094-01-10934-4. URL: https://doi.org/10.1215/S0012-7094-01-10934-4.

[58] A. Kustin, C. Polini, and B. Ulrich. "The equations defining blowup algebras of height three Gorenstein ideals". In: *Algebra Number Theory* 11.7 (2017), pp. 1489–1525. DOI: 10.2140/ant.2017.11.1489. URL: https://doi.org/10.2140/ant.2017.11.1489.

[59] A.R. Kustin, C. Polini, and B. Ulrich. "Rational normal scrolls and the defining equations of Rees algebras". In: *Journal für die reine und angewandte Mathematik (Crelles Journal)* 650 (2011), pp. 23–65. ISSN: 0075-4102. DOI: 10.1515/CRELLE.2011.002.

[60] J.P. Lafon. *Algèbre commutative: langages géométrique et algébrique*. Collection Enseignement des Sciences. Hermann, 1977. ISBN: 9782705658496. URL: https://books.google.fr/books?id=DwnvAAAAMAAJ.

[61] Y. Lai and F. Chen. "Implicitizing rational surfaces using moving quadrics constructed from moving planes". In: *J. Symbolic Comput.* 77 (2016), pp. 127–161. ISSN: 0747-7171. DOI: 10.1016/j.jsc.2016.02.001.

[62] Daniel Lazard. "Computing with parameterized varieties". In: *Algebraic geometry and geometric modeling*. Math. Vis. Springer, Berlin, 2006, pp. 53–69. DOI: 10.1007/978-3-540-33275-6_4. URL: https://doi.org/10.1007/978-3-540-33275-6_4.

[63] T. Luu Ba, L. Busé, and B. Mourrain. "Curve/surface intersection problem by means of matrix representations". In: *SNC Conference*. ACM Press, 2009, pp. 71–78. DOI: 10.1145/1577190.1577205.

[64] D. Manocha and J. Canny. "A new approach for surface intersection". In: *Proceedings of the first ACM symposium on Solid modeling foundations and CAD/CAM applications*. Austin, Texas, United States: ACM, 1991, pp. 209–219. ISBN: 0-89791-427-9. DOI: 10.1145/112515.112544. URL: http://portal.acm.org/citation.cfm?id=112544.

[65] Alexander Morgan and Andrew Sommese. "A homotopy for solving general polynomial systems that respects m-homogeneous structures". In: *Applied Mathematics and Computation* 24.2 (1987), pp. 101 –113. ISSN: 0096-3003. DOI: https://doi.org/10.1016/0096-3003(87)90063-4. URL: http://www.sciencedirect.com/science/article/pii/0096300387900634.

[66] Mircea Mustaţă. "Vanishing theorems on toric varieties". In: *Tohoku Math. J. (2)* 54.3 (Sept. 2002), pp. 451–470. DOI: 10.2748/tmj/1113247605. URL: https://doi.org/10.2748/tmj/1113247605.

[67] V. Neiger and V.T. Xuan. "Computing canonical bases of modules of univariate relations". In: *Proceedings of the 2017 ACM on International Symposium on Symbolic and Algebraic Computation*. ISSAC '17. Kaiserslautern, Germany: ACM, 2017, pp. 357–364. ISBN: 978-1-4503-5064-8. DOI: 10.1145/3087604.3087656.

[68] M. Newman. *Integral Matrices*. Pure and applied mathematics / H. Bass and S. Eilenberg editors. Academic Press, 1972. URL: https://books.google.fr/books?id=1b2WoAEACAAJ.

[69] D. G. Northcott. *Finite Free Resolutions*. Cambridge Tracts in Mathematics. Cambridge University Press, 1976. DOI: 10.1017/CBO9780511565892.

[70] Jasmine Otto, Angus Forbes, and Jan Verschelde. "Solving Polynomial Systems with phcpy". In: (June 2019).

[71] M. Reid and I.R. Shafarevich. *Basic Algebraic Geometry 1*. Springer Berlin Heidelberg, 2013. ISBN: 9783642579080. URL: https://books.google.fr/books?id=U7zuCAAAQBAJ.

[72] F. Russo and A. Simis. "On Birational Maps and Jacobian Matrices". In: *Mathematics Subject Classi¢cations* 126 (Jan. 2000). DOI: 10.1023/A:1017572213947.

[73] T.W. Sederberg and F. Chen. "Implicitization using moving curves and surfaces". In: *Proceedings of SIGGRAPH*. Vol. 29. 1995, pp. 301–308.

[74] T.W. Sederberg, R. Goldman, and H. Du. "Implicitizing rational curves by the method of moving algebraic curves". In: *Journal of Symbolic Computation* 23.2-3 (1997), pp. 153–175. ISSN: 0747-7171. DOI: 10.1006/jsco.1996.0081.

[75] J. Shen, L. Busé, P. Alliez, and N. Dodgson. "A Line/Trimmed NURBS surface intersection algorithm using matrix representations". In: *Computuer Aided Geometric Design* 48.C (Nov. 2016), pp. 1–16. ISSN: 0167-8396. DOI: 10.1016/j.cagd.2016.07.002. URL: https://doi.org/10.1016/j.cagd.2016.07.002.

[76] K. A. Sohn, B. Juttler, M.S. Kim, and W. Wang. "Computing distances between surfaces using line geometry". In: *Computer Graphics and Applications, 2002. Proceedings. 10th Pacific Conference on*. 2002, pp. 236–245. DOI: 10.1109/PCCGA.2002.1167866.

[77] N. Song and R. Goldman. "μ-bases for polynomial systems in one variable". In: *Computer Aided Geometric Design* 26.2 (2009), pp. 217–230. ISSN: 0167-8396. DOI: 10.1016/j.cagd.2008.04.001.

[78] J.B. Thomassen, P. H. Johansen, and T. Dokken. *Closest points, moving surfaces; and algebraic geometry*. Nashboro Press, Brentwood, Tenn, 2005, pp. 351–382.

[79] B. Ulrich and Wolmer V. Vasconcelos. "The equations of Rees algebras of ideals with linear presentation". In: *Mathematische Zeitschrift* 214 (1993), pp. 79–92.

[80] Wolmer V. Vasconcelos. *Arithmetic of Blowup Algebras*. London Mathematical Society Lecture Note Series. Cambridge University Press, 1994. DOI: 10.1017/CBO9780511574726.

[81] Jan Verschelde and Ronald Cools. "Symbolic homotopy construction". In: *Applicable Algebra in Engineering, Communication and Computing* 4.3 (Sept. 1993), pp. 169–183. ISSN: 1432-0622. DOI: 10.1007/BF01202036. URL: https://doi.org/10.1007/BF01202036.

[82] Haohao Wang, Xiaohong Jia, and Ron Goldman. "Axial moving planes and singularities of rational space curves". In: *Computer Aided Geometric Design* 26.3 (2009), pp. 300 –316. ISSN: 0167-8396. DOI: https://doi.org/10.1016/j.cagd.2008.09.002.

[83] Charles A. Weibel. *An Introduction to Homological Algebra*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 1994. DOI: 10.1017/CBO9781139644136.

[84] Lu Yang. "Recent Advances on Determining the Number of Real Roots of Parametric Polynomials". In: *Journal of Symbolic Computation* 28.1 (1999), pp. 225 –242. ISSN: 0747-7171. DOI: https://doi.org/10.1006/jsco.1998.0274. URL: http://www.sciencedirect.com/science/article/pii/S0747717198902747.

[85] W. Zhou, G. Labahn, and A. Storjohann. "Computing minimal nullspace bases". In: *Proceedings of the 37th International Symposium on Symbolic and Algebraic Computation*. ISSAC '12. Grenoble, France: ACM, 2012, pp. 366–373. ISBN: 978-1-4503-1269-1. DOI: 10.1145/2442829.2442881.