HAL
archives-ouvertes.fr

# Implicitization of rational algebraic surfaces with syzygy-based methods

Marc Dohm

▶ To cite this version:

Marc Dohm. Implicitization of rational algebraic surfaces with syzygy-based methods. Mathematics [math]. Université Nice Sophia Antipolis, 2008. English. tel-00294484

HAL Id: tel-00294484
https://tel.archives-ouvertes.fr/tel-00294484

Submitted on 9 Jul 2008

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

UNIVERSITÉ DE NICE - SOPHIA ANTIPOLIS
UFR Sciences

École Doctorale Sciences Fondamentales et Appliquées

# THÈSE

pour obtenir le titre de

**Docteur en Sciences**

de l'Université de Nice - Sophia Antipolis

Spécialité : Mathématiques

présentée et soutenue par

Marc Dohm

# Implicitization of rational algebraic surfaces with syzygy-based methods

Thèse dirigée par André Galligo
soutenue au laboratoire J.A. Dieudonné le 8 Juillet 2008

Membres du jury :

| | | |
|---|---|---|
| M. Laurent Busé | Chargé de Recherche à l'INRIA Sophia Antipolis | Examinateur |
| M. Marc Chardin | Chargé de Recherche à l'Université Pierre et Marie Curie | Rapporteur |
| M. Carlos D'Andrea | Investigador Ramon y Cajal à l'Université de Barcelone | Examinateur |
| M. André Galligo | Professeur à l'Université de Nice | Directeur |
| M. Marc Giusti | Directeur de Recherche à l'Ecole Polytechnique | Président |
| M. Rafael Sendra | Professeur à l'Université d'Alcalá | Rapporteur |

UNIVERSITÉ DE NICE - SOPHIA ANTIPOLIS
UFR Sciences

École Doctorale Sciences Fondamentales et Appliquées

# THÈSE

pour obtenir le titre de

**Docteur en Sciences**

de l'Université de Nice - Sophia Antipolis

Spécialité : Mathématiques

présentée et soutenue par

Marc Dohm

# Implicitization of rational algebraic surfaces with syzygy-based methods

Thèse dirigée par André Galligo
soutenue au laboratoire J.A. Dieudonné le 8 Juillet 2008

Membres du jury :

| | | |
|---|---|---|
| M. Laurent Busé | Chargé de Recherche à l'INRIA Sophia Antipolis | Examinateur |
| M. Marc Chardin | Chargé de Recherche à l'Université Pierre et Marie Curie | Rapporteur |
| M. Carlos D'Andrea | Investigador Ramon y Cajal à l'Université de Barcelone | Examinateur |
| M. André Galligo | Professeur à l'Université de Nice | Directeur |
| M. Marc Giusti | Directeur de Recherche à l'Ecole Polytechnique | Président |
| M. Rafael Sendra | Professeur à l'Université d'Alcalá | Rapporteur |

# Implicitization of rational algebraic surfaces with syzygy-based methods

Marc Dohm

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

# J'aimerais remercier...


- **Laurent Busé** et **André Galligo** pour l'excellent encadrement de ma thèse, pour les bons conseils et pour tout le temps et l'enthousiasme qu'ils ont investis dans ce travail.
- **Marc Chardin** and **Rafael Sendra** qui ont accepté de rapporter cette thèse.
- **Carlos D'Andrea** et **Marc Giusti** d'avoir accepté d'être membres du jury.
- **Nicolás Botbol** et **Alicia Dickenstein** pour les nombreuses discussions lors de notre collaboration, mais surtout pour le chaleureux accueil à Buenos Aires.
- **Severinas Zubė** pour une collaboration fructueuse
- les membres de l'équipe GALAAD de l'INRIA qui m'ont énormément aidé au cours de cette thèse, entre autres **Bernard**, **Mohamed**, **Julien**, **Jean-Pascal**, **Daouda**, **Thi Ha** et **Lionel**.
- **David Cox** pour des explications éclaircissantes
- **Pierre** et **Stéphane** d'avoir rempli notre bureau d'humour et de m'avoir supporté sans jamais se plaindre
- **José, Patrick, Nicolas B., Marcello, Alexandre, Daniel, Philippe, Thu, Delphine, Guillermo, Xavier, Thomas G., Fabien, Asma, Thomas M., Joan, Salissou, Michel, Nicolas R., Olivier, Marie, Julianna, Hugues** pour les bons moments qu'on a partagés.
- tous les autres membres du laboratoire Dieudonné qui font que c'est un endroit aussi agréable, mais qui sont trop nombreux pour les tous nommer ici...
- tous mes amis en dehors du labo et en particulier **Alma**, **Ayşe**, **Zeynep** et **David**.
- und natürlich meiner Mutter **Gerda** und meinem Bruder **Christoph** für ihre Liebe und Unterstützung.

# Contents


Introduction 11

Chapter 1. $\mu$-bases of rational ruled surfaces 19
1. Introduction 19
2. $\mu$-bases of rational planar curves 19
3. Implicitization of rational ruled surfaces with $\mu$-bases 23
4. Algorithm and example 28
5. Remark on the reparametrization of ruled surfaces 31

Chapter 2. Implicitization of canal surfaces 33
1. Introduction 33
2. Modules with two quasi-generators and the $\mu$-basis. 35
3. Elements of Lie and Laguerre sphere geometry 42
4. The isotropic hypersurface and $d$-envelopes 45
5. The dual variety, offsets, and the canal surface. 50
6. Examples and special cases. 54

Chapter 3. Approximation complexes in the bihomogeneous case 57
1. Introduction 57
2. The Segre embedding 58
3. The approximation complex 61
4. Algorithm 69
5. Comments and conclusion 70

Chapter 4. Approximation complexes in the toric case 73
1. Introduction 73
2. Toric embeddings 74
3. Homological tools 79
4. The implicit equation 84
5. The special case $\mathscr{T} = \mathbb{P}^1 \times \mathbb{P}^1$ 84
6. Examples and final remarks 87

Appendix - Implementations and examples 93
A guided example for Chapter 4 93
Surface reparametrization as a preconditioning step 97

Bibliography 99

# Introduction

Il existe plusieurs façons de décrire les surfaces ou courbes algébriques. Les plus communes sont les représentations paramétriques et implicites et le passage entre ces deux représentations est un problème fondamental de la C.A.O. (conception assistée par ordinateur). Dans ce travail, nous traiterons le passage d'une surface parametrée à une description implicite, c'est-à-dire l'implicitisation. Ceci est un problème classique et des nombreuses méthodes d'implicitisation sont connues, bien que toutes coûteuses de point de vue algorithmique. Généralement, ces méthodes sont basées sur les résultants, sur les bases de Gröbner ou bien sur les syzygies. Dans le cadre de ce travail, nous nous intéressons uniquement aux methodes basées sur les syzygies qui ont l'avantage de ne pas calculer l'équation implicite directement, mais qui la présentent comme le déterminant d'une matrice (ou le plus grand diviseur commun de ses mineurs maximaux dans les cas où la matrice n'est pas carrée). Cette représentation matricielle est non seulement plus compacte que l'équation implicite, mais elle permet aussi de résoudre des problèmes géométriques en utilisant les outils performants de l'algèbre linéaire.

Il est connu que pour les courbes rationnelles, il existe toujours une représentation matricielle carrée construite avec des syzygies linéaires. Ceci n'est plus vrai pour les surfaces et si l'on veut représenter une surface par une matrice il y a un choix à faire :

- On veut que la matrice soit carrée, et on sera alors obligé d'utiliser des syzygies quadratiques en plus des syzygies linéaires.
- On utilise exclusivement les syzygies linéaires, et on devra alors se contenter de matrices non-carrées.

La première approche a été développée dans plusieurs contextes différents, par exemple dans [**Co03a**] et [**BCD03**] pour des paramétrisations homogènes ou dans [**AHW05**] pour des paramétrisations bihomogènes. Dans [**KD06**], une généralisation torique de la méthode a été présentée.

Dans ce travail, nous poursuivrons la deuxieme idée, c'est-à-dire que nous essayerons de représenter des surfaces par une matrice construite uniquement avec des syzygies linéaires. Dans [**BJ03**] et [**BC05**]

la validité de cette méthode, qui est basée sur la théorie des complexes d'approximation, a été démontrée pour le cas de surfaces rationnelles données par des paramétrisations homogènes, c'est-à-dire sur $\mathbb{P}^2$. Le but principal de cette thèse est de généraliser la méthode pour des paramétrisations définies sur $\mathbb{P}^1 \times \mathbb{P}^1$ (i.e. des paramétrisations bihomogènes) et, plus généralement, sur une variéte torique quelconque de dimension 2. Nous traiterons aussi quelques classes speciales de surfaces qui permettent une représentation par une matrice carrée. Voici un bref résumé pour chaque chapitre:

Dans le premier chapitre, nous étudierons l'implicitisation des surfaces réglées avec des $\mu$-bases. Nous généraliserons cette méthode déjà connue pour des paramétrisations génériquement injectives au cas général, et nous donnerons des nouvelles preuves. Pour cette classe de surfaces, il existe toujours une représentation par une matrice carrée, qui est une matrice associée au résultant de la $\mu$-base, par exemple la matrice de Bézout ou la matrice de Sylvester.

Dans le deuxième chapitre, une autre classe de surfaces est étudiée - les surfaces canales. Ces surfaces, qui sont très souvent utilisées dans la C.A.O., sont données comme l'enveloppe d'une famille de sphères. Nous les relierons à certaines surfaces en dimension supérieure avec des propriétés similaires à celles des surfaces réglées. Ensuite, nous verrons que l'on peut généraliser les méthodes du premier chapitre et que cela nous permet de trouver une représentation de la surface comme la matrice à un résultant également.

Le troisième chapitre constitue un premier pas vers la généralisation de la méthode des complexes d'approximation : nous montrerons qu'une surface donnée par une paramétrisation bihomogène de bidegré $(d, d)$ peut être représentée par une matrice (non-carrée) construite exclusivement avec des syzygies linéaires.

Dans le quatrième chapitre, cette méthode sera dévéloppée dans le contexte beaucoup plus général de paramétrisations sur des variétés toriques (dont les paramétrisations homogènes et bihomogènes sont des cas spéciaux). Cette généralisation rend nécessaire l'emploi de plusieurs outils théoriques de l'algèbre commutative combinatoire, mais nous verrons que l'utilisation de variétés toriques améliore de façon importante la performance de la méthode et la taille des matrices de représentation.

Enfin, dans l'appendice, nous expliquerons dans un exemple comment la matrice de représentation peut être calculée avec le logiciel Macaulay2. De plus, nous montrerons que dans certains cas une reparamétrisation de la surface peut optimiser la méthode.

Rational algebraic curves and surfaces can be described in several different ways, the most common being parametric and implicit representations. Parametric representations describe the geometric object as the image of a rational map, whereas implicit representations describe it as the set of points verifying a certain algebraic condition, e.g. as the zeros of a polynomial equation. Both representations have a wide range of applications in Computer Aided Geometric Design (CAGD), and depending on the problem one needs to solve, one or the other might be better suited. To give a simple example, the parametric description is better for drawing a surface, as it allows to rapidly generate points on the surface, which can then be interpolated, whereas an implicit representation is better adapted for testing if a given point lies on the surface, since one only needs to check whether the point verifies the algebraic condition that defines the surface. It is thus interesting to be able to pass from one representation to the other. In this thesis we will study the implicitization problem, i.e. finding the implicit equation of an algebraic curve or surface defined parametrically. This is a classical problem and there are numerous approaches to its solution, most of them based either on resultants, Gröbner bases, or syzygies. A good historical overview of methods based on resultants or Gröbner bases can be found in [**SC95**] and [**Co01**]; our focus will be on syzyzgy-based methods. We will study such methods in several different contexts in order to implicitize certain classes of rational algebraic surfaces.

To motivate this approach, let us give a brief historical overview. The theory of syzygies has been developed in the more theoretical context of commutative algebra at the beginning of the 20th century by mathematicians such as David Hilbert. However, it was only in the 1990s that the CAGD and geometric modeling community discovered that the concept of syzygies is useful in their field. Initially unaware of the connections to commutative algebra, [**SC95**], [**SSQK94**], [**SGD97**], and numerous other authors labeled this approach the method of "moving curves" (or "moving surfaces") and showed how it can be used to express the implicit equation as a determinant. In the case of planar rational curves, i.e. for parametrizations of the form

$$\begin{array}{ccc} \mathbb{A}^1 & \overset{\phi}{\dashrightarrow} & \mathbb{A}^2 \\ s & \mapsto & \left(\dfrac{f_1(s)}{f_3(s)}, \dfrac{f_2(s)}{f_3(s)}\right) \end{array}$$

where $f_i \in \mathbb{K}[s]$ are polynomials of degree $d$ such that $\gcd(f_1, f_2, f_3) = 1$ and $\mathbb{K}$ is a field, a linear syzygy (or moving line) is a linear relation on the polynomials $f_1, f_2, f_3$, i.e. a linear form $L = g_1T_1 + g_2T_2 + g_3T_3$ in the variables $T_1, \ldots, T_3$ and with polynomial coefficients $g_i \in \mathbb{K}[s]$ such

that

$$\sum_{i=1,\dots,3} g_i f_i = 0$$

We denote by $\mathrm{Syz}(\phi)$ the set of all those linear syzygies forms and for any integer $\nu$ the graded part $\mathrm{Syz}(\phi)_\nu$ of syzygies of degree $\nu$. It is obvious that $\mathrm{Syz}(\phi)_\nu$ is a finite-dimensional $\mathbb{K}$-vector space with a certain basis $(L_1, \dots, L_k)$, which can easily be obtained by solving a linear system. We define the matrix $M_\nu$ of coefficients of the $L_i$ as

$$M_\nu = \begin{pmatrix} L_1 & L_2 & \cdots & L_k \end{pmatrix},$$

that is, the coefficients of the syzygies $L_i$ (with respect to a $\mathbb{K}$-basis of $\mathbb{K}[s]_\nu$) into the columns of the matrix. Note that the entries of this matrix are linear forms in the variables $T_1, T_2, T_3$ with coefficients in the field $\mathbb{K}$. Let $F$ denote the homogeneous implicit equation of the curve and $\deg(\phi)$ is the degree of the parametrization (Intuitively, $\deg(\phi)$ measures how many times the curve is traced). It is known that

- If $\nu = d-1$, then $M_\nu$ is a square matrix, such that $\det(M_\nu) = F^{\deg(\phi)}$.
- If $\nu \geq d$, then $M_\nu$ is a non-square matrix with more columns than rows, such that the greatest common divisor of its minors of maximal size equals $F^{\deg(\phi)}$.

In other words, one can always represent the curve as a square matrix of linear syzygies. In principle, one could now actually calculate the implicit equation, however, it might be advantageous to avoid the costly determinant computation and work directly with the matrix instead, as it has the advantage of representing the curve in a much more compact form than the implicit equation and as it makes the well-developed theory and tools of linear algebra applicable to solve geometric problems. For instance, testing whether a point $P$ lies on the curve only requires computing the rank of $M_\nu$ evaluated in $P$. This rank drops if and only if the point lies on the curve. Other interesting results using square matrix representations directly to solve geometric problems are presented, for example, in [**ACGS07**] or [**Ma94**], in which intersection problems are treated by means of eigenvalue techniques.

It is a natural question whether this kind of matrix representation can be generalized to rational surfaces defined as the image of a map

$$\begin{array}{ccc} \mathbb{A}^2 & \overset{\phi}{\dashrightarrow} & \mathbb{A}^3 \\ (s,t) & \mapsto & \left(\dfrac{f_1(s,t)}{f_4(s,t)}, \dfrac{f_2(s,t)}{f_4(s,t)}, \dfrac{f_3(s,t)}{f_4(s,t)}\right) \end{array}$$

where $f_i \in \mathbb{K}[s,t]$ are polynomials of degree $d$ such that $\gcd(f_1, \dots, f_4) = 1$. In this case, a linear syzygy (or moving plane) of the parametrization $\phi$ is a linear relation on the polynomials $f_1, \dots, f_4$, i.e. a linear

form $L = g_1T_1 + g_2T_2 + g_3T_3 + g_4T_4$ in the variables $T_1, \ldots, T_4$ with $g_i \in \mathbb{K}[s,t]$ such that

$$\sum_{i=1,\ldots,4} g_i f_i = 0$$

Exactly in the same way as for curves, one can set up the matrix $M_\nu$ of coefficients of the syzygies in a certain degree $\nu$, but unlike in the curve case, it is in general not possible to choose a degree $\nu$ such that $M_\nu$ is a square matrix representation of the surface. But before dealing with this problem, let us first define clearly what we mean by "matrix representation". We state the definition for arbitrary dimension, the case $n = 2$ corresponds to curves and the case $n = 3$ to surfaces.

DEFINITION 0.1. Let $\phi$ be a rational parametrization of a hypersurface $\mathscr{S} \subset \mathbb{A}^n$ with homogeneous implicit equation $F \in \mathbb{K}[T_0, \ldots, T_n]$. A matrix $M$ with entries in the polynomial ring $\mathbb{K}[T_0, \ldots, T_n]$ is called a *representation matrix* of $\phi$ if

- $M$ is generically of full rank,
- the rank of $M$ evaluated in a point of $\mathbb{A}^n$ drops if and only if the point lies on the hypersurface,
- the greatest common divisor of all minors of $M$ of maximal size equals $F^{\deg(\phi)}$.

Note that if $M$ is square then the gcd in the third bullet point is just the determinant of $M$. As we have said above, it is not always possible to obtain a square matrix representation constructed exclusively with linear syzygies. In recent years, two main approaches have been proposed to deal with this problem

- One allows the use of quadratic syzygies (or higher-order syzygies) in addition to the linear syzygies in order to be able to construct square matrices.
- One only uses linear syzygies as in the curve case and obtains non-square representation matrices.

At this point, we should also remark that for several reasons we will explain later, it is usually necessary to homogenize the parametrization $\phi$, i.e. consider it as a projective map. For example, in the surface case, one often considers $\phi$ as a map $\mathbb{P}^2 \dashrightarrow \mathbb{P}^3$ or as a map $\mathbb{P}^1 \times \mathbb{P}^1 \dashrightarrow \mathbb{P}^3$. For example, the first approach using linear and quadratic syzygies (or moving planes and quadrics) has been treated in [**Co03a**] for base-point-free homogeneous parametrizations, and [**BCD03**] does the same for parametrizations with base points. In [**AHW05**], square matrix representations of bihomogeneous parametrizations are constructed with linear and quadratic syzygies, whereas [**KD06**] gives such a construction in the toric case (i.e. for parametrizations defined on toric varieties of dimension 2).

As remarked before, square matrix representations have already been used to solve geometric problems without computing the implicit equation. For non-square matrices, this has yet to be done and there are first promising attempts to generalize such applications for non-square matrices. The reason why this is interesting is because as we will see, the second approach which only uses linear syzygies has certain advantages. For instance, linear syzygies are much easier to compute than higher-order syzygies, namely by solving a linear system. Moreover, the methods using quadratic syzygies usually require more restrictive conditions on the parametrization and the choice of the quadratic syzygies is often not canonical.

In this thesis we will focus on the construction of non-square matrix representations with linear syzygies. This has been solved in [**BJ03**] and [**BC05**] for homogeneous parametrizations; the results obtained are valid in a very general setting and are based on the use of theoretical tools from homological algebra, notably the so-called approximation complexes. The main objective of this work is to generalize those results to the cases of bihomogeneous and toric parametrizations (Chapter 3 and 4), but we also treat two special classes of rational surfaces - ruled surfaces and canal surfaces - for which it is actually possible to obtain square representation matrices only with linear syzygies (Chapter 1 and 2). Let us sum up briefly the contents of each chapter.

Chapter 1 treats a special class of rational surfaces: rational ruled surfaces. These surfaces can be defined by a parametrization which is linear in one of the variables. In [**CZS01**] and subsequent publications, it has been shown that for a ruled surface defined by a generically injective parametrization one can define a so-called $\mu$-basis consisting of two syzygies $(p, q)$ and that the resultant $\mathrm{Res}(p, q)$ equals the implicit equation of the surface. First, we recall the corresponding theory of $\mu$-bases for rational planar curves and give some new proofs of the key results by using a reparametrization argument. Then we proceed to establish a geometric connection between the ruled surface and its associated Plücker curve, which allows us to generalize the theory to ruled surfaces defined by non-injective parametrizations. In particular, we shall see that for this class of surfaces, it is possible to give a square representation matrix of linear syzygies, which is a matrix associated to the resultant of the $\mu$-basis, e.g. the Sylvester or Bézout matrix. Also, we deal with a problem of finding a proper reparametrization of a ruled surface, for which we give a solution in a special case.

The subject of Chapter 2 are canal surfaces, another special class of surfaces very popular for geometric modeling. They are defined as the envelope of a family of spheres moving along a space curve. However, the classical definition of the envelope leads to the apparition of counterintuitive extraneous components. Using Lie and Laguerre sphere geometry, we relate the canal surface (and its offsets) to certain surfaces in four-dimensional projective space which are defined by the resultant of two linear forms. These surfaces have similar properties as the ruled surfaces from the first chapter, and we develop a multi-dimensional generalization of the notion of the $\mu$-basis and propose an efficient algorithm for its computation. This approach allows us to eliminate the extraneous factors of the envelope and to represent the canal surface (and its offsets) by a square matrix associated to the resultant of the $\mu$-basis.

In Chapter 3, we make a first step towards the generalization of the method of approximation complexes introduced in [**BJ03**] and [**BC05**] for homogeneous parametrizations. We consider a rational surface defined by a bihomogeneous parametrization of bidegree $(d, d)$ and transform the bigraded structure of the map into a singly graded one by embedding $\mathbb{P}^1 \times \mathbb{P}^1$ in a hypersurface in $\mathbb{P}^3$ via the Segre embedding. Algebraically, this means that we have to generalize the results obtained in the above papers for a quotient ring $A$ instead of a polynomial ring, in particular we need to compute bounds on the local cohomology of this ring and the symmetric algebra $\mathrm{Sym}_A(I)$, where $I = (f_1, \ldots, f_4)$. We show that for any $\nu \geq 2d-1-\mathrm{indeg}(I^{\mathrm{sat}})$, the matrix $M_\nu$ as defined above is a non-square matrix representation, which can be computed by solving a linear system.

In Chapter 4 we generalize the results of the third chapter to parametrizations over a two-dimensional toric variety $\mathscr{T}$, which includes homogeneous and bihomogeneous parametrizations as special cases. The basic idea is similar to what we have seen before, but instead of the Segre embedding we use a more general toric embedding to consider the variety as a surface in a high-dimensional projective space. Contrary to the third chapter, it will almost never be a hypersurface. On the algebraic side, this means that we have to work over more complicated rings than before, i.e. quotient rings of the form $A = \mathbb{K}[X_0, \ldots, X_m]/J$, where $J$ is a toric ideal. These ideals have a very rich and interesting combinatorial structure, which we will study in detail. Using tools of combinatorial commutative algebra, we will generalize the method of approximation complexes to this very general setting by deriving new bounds on local cohomology and by giving new proofs for certain results. We then make explicit the constructions for the particularly important case $\mathscr{T} = \mathbb{P}^1 \times \mathbb{P}^1$. Finally, we give numerous examples to

illustrate how these new results can be used to fully exploit the combinatorial structure of a given parametrization and show that this a major improvement in terms of computation time as well as in terms of the size of the representation matrices.

A commented implementation of the method is included in the Appendix to illustrate how to compute a matrix representation with the computer algebra system Macaulay2 [**M2**]. Furthermore, we explain that in certain cases it can be advisable to perform a surface reparametrization as a preconditioning step in order to simplify computations and decrease the size of the representation matrices.

CHAPTER 1

# $\mu$-bases of rational ruled surfaces

Abstract. Chen, Sederberg, and Zheng introduced the notion of a $\mu$-basis for a rational ruled surface in [**CZS01**] and showed that its resultant is the implicit equation of the surface, if the parametrization is generically injective. We generalize this result to the case of an arbitrary parametrization of a rational ruled surface. We also give a new proof for the corresponding theorem in the curve case and treat the reparametrization problem for curves and ruled surfaces. In particular, we propose a partial solution to the problem of computing a proper reparametrization for a rational ruled surface. The results in this chapter have been accepted for publication in [**Do06**].

## 1. Introduction

Ruled surfaces are frequently used for modeling purposes in Computer Aided Geometric Design and in several applications, e.g. the computation of the intersection of two ruled surfaces, see [**FGN05**], it is necessary to implicitize such surfaces. The method of $\mu$-bases (also known as "moving lines" or "moving surfaces") constitutes an efficient solution to the implicitization problem for ruled surfaces. Introduced in 1998 by Cox, Sederberg, and Chen for rational curves in [**CSC98**], it was generalized to ruled surfaces in [**CZS01**] and [**CW03b**]. Whereas the curve case is very well understood and we know that the resultant of a $\mu$-basis is the implicit equation to the power $d$, where $d$ is the degree of the rational map induced by the parametrization, this result is still to be shown in its full generality (i.e. for arbitrary $d$) for ruled surfaces. We fill this gap by giving a proof, which relies on a geometric idea that reduces the ruled surface case to the curve case. From a computional point of view, $\mu$-bases are in general more efficient than other resultant-based methods such as the ones introduced in [**BC05**] or in [**Kh03**], since they are well adapted to the geometry of ruled surfaces and produce small representation matrices.

## 2. $\mu$-bases of rational planar curves

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

a parametrization map

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

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

$$\begin{array}{rcl} \mathrm{Syz}(f_0,f_1,f_2) & = & \{P \in \mathrm{R}[x,y,z] \mid \deg(P) \le 1, P(f_0,f_1,f_2) = 0\} \\ & \subseteq & \mathrm{R}[x,y,z] \end{array}$$

Then we have the following well-known result.

THEOREM 1.1. *There exists an isomorphism of graded* R*-modules*

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

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

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

The isomorphism in the above theorem is a direct consequence of the Hilbert-Burch Theorem (see [**Ei95**, Th. 20.15]) applied to the exact sequence

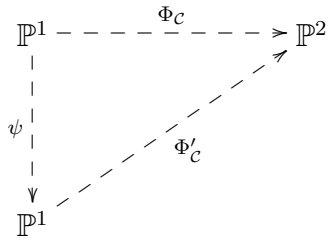
$$0 \to \mathrm{Syz}(f_0,f_1,f_2)(-n) \to \mathrm{R}^3(-n) \to \mathrm{R} \to \mathrm{R}/I \to 0$$

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

DEFINITION 1.2. A basis $(p,q)$ of $\mathrm{Syz}(f_0,f_1,f_2)$ with minimal degrees $\deg(p) = \mu_1$ and $\deg(q) = \mu_2$ in $s$ and $\bar{s}$ is called a $\mu$-basis of the parametrization $\Phi_{\mathcal{C}}$.

One interesting feature of $\mu$-bases is that the resultant of its elements is a power of the implicit equation of $\mathcal{C}$, as was proved in [**CSC98**, Sect. 4, Th. 1]. We propose an alternative proof which relies on the idea that we can reduce the problem to the generically injective case. The essential tool for this reduction is the existence of a proper reparametrization, which is a consequence of Lüroth's Theorem, a proof of which can be found for example in [**vdW70**, Section 5.4]. In the following lemma we deduce a reparametrization with an additional property.

LEMMA 1.3. *There exists* $\psi : \mathbb{P}^1 \dashrightarrow \mathbb{P}^1$ *parametrized by two coprime homogeneous polynomials* $h_0$ *and* $h_1$ *of degree* $\deg(\Phi_{\mathcal{C}})$ *and a parametrization* $\Phi'$ *of* $\mathcal{C}$ *defined by homogeneous polynomials* $f_0'(s,\bar{s})$, $f_1'(s,\bar{s})$ *and* $f_2'(s,\bar{s})$ *such that the following diagram commutes:*




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

PROOF. First, we treat the case $\gcd(f_0, f_2) = \gcd(f_1, f_2) = 1$. Then we can dehomogenize $\frac{f_0}{f_2}$ and $\frac{f_1}{f_2}$ by setting $\bar{s} = 1$ without changing the degree as rational functions and decompose them by means of Lüroth's Theorem [**vdW70**, Section 5.4]) in the following way

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

with $\gcd(h_0, h_1) = \gcd(f'_0, f'_2) = \gcd(f'_1, \tilde{f}'_2) = 1$ and $\deg(h_i) = \deg(\Phi_{\mathcal{C}})$ for $i \in \{0, 1\}$ after having rehomogenized them with respect to $\bar{s}$. By multiplying the fractions with a suitable power of $h_1$ we can consider the $f'_i$ as bivariate homogeneous polynomials

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

Then the numerators and denominators are all coprime, which for the right hand sides follows from [**Zi91**, Prop. 6] and we deduce the term-by-term equalities $f_i = f'_i(h_0, h_1)$ for $i \in \{0, 1, 2\}$.

In the general case, we divide the polynomials of the parametrization by their greatest common divisor and perform a generic coordinate change in order to pass to another parametrization of $\mathcal{C}$ which fulfills $\gcd(f_0, f_2) = \gcd(f_1, f_2) = 1$ and whose polynomial decomposition completes the commutative diagram of rational maps. □

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

THEOREM 1.4. *Let $(p, q)$ be a $\mu$-basis of the parametrization $\Phi_{\mathcal{C}} : \mathbb{P}^1 \dashrightarrow \mathbb{P}^2$. Then*

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

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

*resultant of $p$ and $q$, e.g. the Bézout or Sylvester matrix, is a square representation matrix of the curve $\mathcal{C}$.*

PROOF. First of all, we may assume that $\gcd(f_0, f_2) = \gcd(f_1, f_2) = 1$ (if necessary, we divide by $\gcd(f_0, f_1, f_2)$ and perform a generic coordinate change, both of which do not affect the result). So by Lemma 1.3 there exist $f_0', f_1', f_2' \in \mathrm{R}$ and homogeneous, coprime $h_0, h_1 \in \mathrm{R}$ of degree $\deg(\Phi_{\mathcal{C}})$, such that

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

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

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

for some constant $\lambda \neq 0$ and a homogeneous $a \in \mathrm{R}$ of degree $\deg(q) - \deg(p)$. (If $\mu_1 = \mu_2$, we have $p' \circ h = \alpha_1 p + \alpha_2 q$ and $q' \circ h = \beta_1 p + \beta_2 q$ for some constants $\alpha_i$ and $\beta_i$ (see [**CW03a**, Th. 2]), which leads to computations that are analogous to the ones that follow).

Now we can apply elementary properties of resultants to calculate

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

where $c = \lambda^{-\mu_2} \cdot \mathrm{Res}(h_0, h_1) \in \mathbb{K}^*$ is a constant (since the $h_i$ do not depend on $x, y, z$) and non-zero (because $\gcd(h_0, h_1) = 1$). The third identity is a well-known base change formula for resultants, which is proved in [**Jo91**, 5.12], and in the last identity we used $\deg(h_0) = \deg(\Phi_{\mathcal{C}})$.

So by (1) we have reduced the theorem to the special case where the parametrization has degree 1, and it remains to show:

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

a) Suppose $p = G \cdot H$ were reducible into non-constant $G, H \in \mathrm{R}[x, y, z]$, then one of the two, say $G$, would be independent of $x, y, z$, because $p$ is linear in those variables and $H$ would define a syzygy with lower degree than $p$ which contradicts the definition of a $\mu$-basis. So $p$ is irreducible in $\mathrm{R}[x, y, z]$ and $\mathrm{Res}(p, q) = 0$ would mean that $q = r \cdot p$

with $r \in \mathrm{R}$, which is impossible, for $p$ and $q$ are linearly independent over R. Hence $\mathrm{Res}(p,q) \neq 0$ and by (1) also $\mathrm{Res}(p',q') \neq 0$.

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

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

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

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

□

## 3. Implicitization of rational ruled surfaces with $\mu$-bases

Chen, Sederberg, and Zheng introduced the notion of a $\mu$-basis for rational ruled surfaces in [**CZS01**], and it was further developed in [**CW03b**]. However, they worked with the restrictive assumption that the parametrization is generically injective. In this section, we will give a proof for the ruled surface version of Theorem 1.4 in its general form and explain to what extent the ruled surface case can be reduced to the curve case.

In this chapter, a rational ruled surface $\mathcal{S}$ is meant to be a surface given by a rational map

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

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

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

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

Let us fix some notation first: Let $\mathrm{R} = \mathbb{K}[s,\bar{s}]$ and define the R-module of syzygies on $f_0,\ldots,f_3$ depending only on $s$ and $\bar{s}$ as

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

Then the structure of this module is well known; see [**CZS01**] for a proof of the following

THEOREM 1.5. *There exists an isomorphism of graded* R*-modules*

$$\mathrm{Syz}_{\mathrm{R}}(f_0,\ldots,f_3) \cong \mathrm{R}(-\mu_1) \oplus \mathrm{R}(-\mu_2)$$

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

DEFINITION 1.6. A basis $(q_1, q_2)$ of $Syz_{\mathrm{R}}(f_0, f_1, f_2, f_3)$ where $q_1$ and $q_2$ are homogeneous of minimal degrees $\deg(q_1) = \mu_1$ and $\deg(q_2) = \mu_2$ in $s$ and $\bar{s}$ is called a $\mu$-basis of the parametrization $\Phi_{\mathcal{S}}$.

As we can see, the syzygy module of the surface $\mathcal{S}$ resembles the one of a curve, which leads to the following question: is there a curve with the same syzygy module which can be defined by means of the surface parametrization? The answer to this question is positive and according to an idea due to [**BEG07**], we define the curve $\mathcal{C}$ associated to $\mathcal{S}$ by

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

where $p_{ij} := f_{i0}f_{j1} - f_{i1}f_{j0} \in \mathrm{R}$ are the Plücker coordinates, which are homogeneous of degree $n_1 + n_0$. Let us denote $g := \gcd(p_{03}, p_{13}, p_{23})$.

The geometric idea behind this definition is that for almost all parameter values $(s:\bar{s}) \in \mathbb{P}^1$ the image of the map

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

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

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

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

LEMMA 1.7. *If* $\gcd(f_{30}, f_{31}) = 1$ *then*

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

PROOF. Let us suppose $q = \gcd(p_{03}, p_{13}, p_{23}) \neq 1$; the case $q = 1$ is trivial. We need to show that $q$ divides the other Plücker coordinates

as well. Euclidean division of the $f_{ij}$ by $q$ yields

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

We have the congruences

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

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

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

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

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

Proposition 1.8 (Degree Formula). *With the same notation and hypotheses as before the equality*

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

*holds.*

Proof. This formula is an adaptation of the general result

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

(see [**Fu84**, Prop. 4.4] for a proof, $m_p$ is the multiplicity of $p$). Our formula follows by counting the base points $\sum_{p \in V(I)} m_p = \deg(g) + (n_1 - n_0)$, where $n_1 - n_0$ is the trivial multiplicity of the base point $(\infty, 0) := ((1:0),(0:1))$ and where the other base points (including additional multiplicities of $(\infty, 0)$) can be identified with the roots of $g$ by elementary calculations. □

Note that for characteristic zero $\deg(\Phi_{\mathcal{S}})$ - and thus also $\deg(\mathcal{S})$ - can be computed by means of gcd and resultant computations, see [**PS06**].

Next, we proceed to relate $\mathrm{Syz}_{\mathrm{R}}(f_0, \ldots, f_3)$ to the syzygy module of the associated curve, given as

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

PROPOSITION 1.9. *If* $\gcd(f_{30}, f_{31}) = 1$*, then there exists a canonical isomorphism of graded* R*-modules*

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

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

PROOF. As a direct consequence of Theorem 1.1 and the degree formula, we obtain

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

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

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

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

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

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

$$\begin{aligned} \varphi : \quad \mathrm{Syz}_{\mathrm{R}}(f_0, \ldots, f_3) &\to \mathrm{Syz}(p_{03}, p_{13}, p_{23}) \\ h_0x + h_1y + h_2z + h_3w &\mapsto h_0x + h_1y + h_2z \end{aligned}$$

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

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

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

$$hf_{30} = h_0f_{00} + h_1f_{10} + h_2f_{20} \tag{4}$$

and by substituting this in the above equation also $hf_{31} = h_0f_{01} + h_1f_{11} + h_2f_{21}$. These two relations show that $h_0x + h_1y + h_2z - hw \in \mathrm{Syz}_{\mathrm{R}}(f_0, \ldots, f_m)$ is a preimage of $h_0x + h_1y + h_2z$, hence $\varphi$ is surjective and the proof is complete. □

COROLLARY 1.10. *If we perform a generic coordinate change beforehand, we also have* $\deg(\mathcal{S}) = \deg(\mathcal{C})$ *and* $\deg(\Phi_{\mathcal{S}}) = \deg(\Phi_{\mathcal{C}})$ *in the situation of the preceding Proposition 1.9.*

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

An important remark is that the inverse $\varphi^{-1}$ of $\varphi$ in the proof of Proposition 1.9 can be described explicitly as

$$\begin{array}{rcl} \mathrm{Syz}(p_{03}, p_{13}, p_{23}) & \to & \mathrm{Syz}_{\mathrm{R}}(f_0, \ldots, f_3) \\ h_0x + h_1y + h_2z & \mapsto & h_0x + h_1y + h_2z - \dfrac{h_0f_{00} + h_1f_{10} + h_2f_{20}}{f_{30}}w \end{array} \tag{5}$$

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

One can regard the results in Theorem 1.5 as a corollary of Theorem 1.1 and Proposition 1.9. Let us also note that Theorem 1.1 and Theorem 1.5 can easily be generalized to higher dimension and the proofs are completely analogous to the ones given here. For example, the $\mu$-basis of a curve in $\mathbb{P}^m$ consists of $m-1$ syzygies whose degrees in $s$ and $\bar{s}$ sum up to $d$. We are now ready to show our main result.

THEOREM 1.11. *Let $(q_1, q_2)$ be a $\mu$-basis of the parametrization $\Phi_{\mathcal{S}} : \mathbb{P}^1 \times \mathbb{P}^1 \dashrightarrow \mathbb{P}^3$. Then*

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

*where $F_{\mathcal{S}}$ is an implicit equation of the ruled surface $\mathcal{S}$ and where the resultant is taken with respect to $s$ and $\bar{s}$. In particular, any matrix associated to the resultant of $q_1$ and $q_2$, e.g. the Bézout or Sylvester matrix, is a square representation matrix of the ruled surface $\mathcal{S}$.*

PROOF. First, we can ensure that the hypotheses of Proposition 1.9 are fulfilled by performing a generic linear coordinate change in $\mathbb{P}^1 \times \mathbb{P}^1$, which leaves both the implicit equation and the resultant unchanged (up to multiplication by a constant). We will show that $\mathrm{Res}(q_1, q_2)$ is the power of an irreducible polynomial, i.e. that it defines an irreducible hypersurface in $\mathbb{P}^3$. Let us consider the incidence variety $\mathcal{W} := \{( (s_0 : \bar{s_0}), (x_0 : y_0 : z_0 : w_0)) \in \mathbb{P}^1 \times \mathbb{P}^3 \mid q_i(s_0, \bar{s_0}, x_0, y_0, z_0, w_0) = 0 \}$ then we have the following diagram

$$\begin{array}{ccc} \mathcal{W} & \xrightarrow{\quad\pi_2\quad} & \mathbb{P}^3 \\ {\scriptstyle \pi_1}\downarrow & & \\ \mathbb{P}^1 & & \end{array}$$

where $\pi_1$ and $\pi_2$ are the canonical projections. $\mathcal{W}$ is a vector bundle over $\mathbb{P}^1$, as the $q_i$ are linear in $x, y, z$, and $w$, and for any parameter $(s_0 : \bar{s_0})$ the fiber is a $\mathbb{K}$-vector space of codimension 2, because $q_1(s_0, \bar{s_0})$ and

$q_2(s_0, \bar{s_0})$ are linearly independent, as was proved in [**CW03b**, Sect. 2, Prop. 3]. We will give a proof of this fact in a more general setting in Proposition 2.9.

As $\mathbb{P}^1$ is irreducible, it follows that $\mathcal{W}$ is irreducible too (see [**Sh77**, Ch.6, Th.8]), hence so is $\mathrm{Im}(\pi_2)$. (If $\mathrm{Im}(\pi_2) = A \cup B$ for two closed sets $A$ and $B$, $\mathcal{W} = \pi_2^{-1}(A) \cup \pi_2^{-1}(B)$, which implies $\mathcal{W} = \pi_2^{-1}(A)$ or $\mathcal{W} = \pi_2^{-1}(B)$, since $\mathcal{W}$ is irreducible and, consequently, $\mathrm{Im}(\pi_2) = A$ or $\mathrm{Im}(\pi_2) = B$). Now the points of $\mathrm{Im}(\pi_2)$ are exactly those for which the $q_i$ have a common zero in $s$ and $\bar{s}$, so by definition of the resultant they are the zeros of $\mathrm{Res}(q_1, q_2)$. In other words, we have shown that $V(\mathrm{Res}(q_1, q_2)) = \mathrm{Im}(\pi_2)$ is irreducible, so $\mathrm{Res}(q_1, q_2)$ is the power of an irreducible polynomial.

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

In the proof of Theorem 1.9, we have seen the isomorphism of R-modules

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

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

As remarked earlier on, $\varphi$ takes $\mu$-bases to $\mu$-bases, so $(\varphi(q_1), \varphi(q_2))$ is a $\mu$-basis of $\Phi_{\mathcal{C}}$. Applying Theorem 1.4 yields

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

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

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

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

## 4. Algorithm and example

In this section, we give a detailed description of a new algorithm to compute a $\mu$-basis of a rational ruled surface based on the one-to-one correspondence between the syzygies of a ruled surface and its associated curve: As we have remarked, a $\mu$-basis of the ruled surface can be obtained by computing a $\mu$-basis of its associated curve (e.g.

with the algorithm presented in [**CW03a**]) and taking its image under the isomorphism (5) in the proof of Proposition 1.9. In particular, this method has the same computational complexity as the curve algorithm that is used (since all the other steps in the algorithm are immediate), which makes it very efficient.

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

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

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

ALGORITHM ($\mu$-basis of a ruled surface)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

and we obtain

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

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

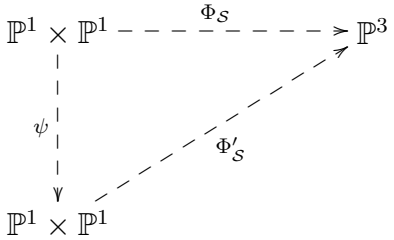
We have seen and used the equality $\deg(\Phi_{\mathcal{C}})\cdot\deg(\mathcal{C}) = \deg(\Phi_{\mathcal{S}})\cdot\deg(\mathcal{S})$ between the surface $\mathcal{S}$ and its associated curve $\mathcal{C}$. It is natural to ask whether $\deg(\mathcal{C}) = \deg(\mathcal{S})$ also holds. However, this is not true in our example: we have $\deg(\mathcal{C}) = 2$, but $\deg(\mathcal{S}) = 4$. According, to the corollary to Proposition 1.9, we would have had to perform a generic coordinate change in order to ensure the equality of the degrees.

Let us compare the $\mu$-basis method to some others. In our example, $F_{\mathcal{S}}^2$ is obtained as a determinant of a $8\times 8$-matrix, the Sylvester matrix of $q_1$ and $q_2$. After dehomogenizing our surface and homogenizing back to $\mathbb{P}^2$ we can use approximation complexes to implicitize as in [**BC05**], compare also Chapters 3 and 4, and we obtain $F_{\mathcal{S}}^2$ as the quotient of a $28\times 28$-determinant by a $12\times 12$-determinant and an additional term that arises because we add a non-complete-intersection base point when passing from $\mathbb{P}^1\times\mathbb{P}^1$ to $\mathbb{P}^2$, which is by far not as efficient.

Another possibility is to use the classical formula $F_{\mathcal{S}}^2(w=1) = \mathrm{Res}(f_0 - xf_3, f_1 - yf_3, f_2 - zf_3)$ combined with an efficient method to calculate the resultant such as [**Kh03**]. $F_{\mathcal{S}}^2$ is obtained as the determinant of $10\times 10$-matrix, which is larger than our Sylvester matrix and whose entries are themselves determinants of smaller matrices.

## 5. Remark on the reparametrization of ruled surfaces

In the proof of Theorem 1.4 about the implicit equation of a planar curve, we reduced the general case to the proper case by reparametrizing the curve. If the field $\mathbb{K}$ is of characteristic zero, we know by the theorem of Castelnuovo that there exists a proper reparametrization for any rational surface, i.e. there exists a commutative diagram




where $\psi = (\sigma,\tau)$ is of degree $\deg(\mathcal{S})$ and $\Phi'_{\mathcal{S}}$ is a proper reparametrization of $\mathcal{S}$. As far as we know, this problem is yet to be solved algorithmically. However, [**Pe06**] gives a criterion for the existence of a reparametrization of a rational surface such that $\sigma = \sigma(s,\bar{s})$ depends only on $s$ and $\bar{s}$ and $\tau = \tau(t,\bar{t})$ depends only on $t$ and $\bar{t}$ and proposes an algorithm for its computation if it exists. If we restrict our attention to ruled surfaces we can also treat the case where $\tau = (\bar{t}\alpha + t\beta, \bar{t}\gamma + t\delta)$

with $\alpha, \beta, \gamma, \delta \in \mathbb{K}[s, \bar{s}]$ such that $\alpha\delta - \beta\gamma \neq 0$ by using the associated curve. So let us suppose that there exists a reparametrization such that we can write

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

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

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

from which we conclude that $\sigma$ yields a proper reparametrization of the associated curve in the generic case $\deg(\Phi_{\mathcal{S}}) = \deg(\Phi_{\mathcal{C}})$. On the other hand, any $\lambda(s, \bar{s})$ defining a proper reparametrization $p_i = p''_i(\lambda)$ of $\mathcal{C}$ differs from $\sigma$ only by a homography, so we can assume $\lambda = \sigma$, which provides us with a (naive) method for calculating the reparametrization: We compute $\sigma$ with a reparametrization algorithm for curves such as in [**Pe06**] and consider (6) as a linear system of equations by comparing the coefficients of the left hand side and the right hand side, where we leave the coefficients of $\alpha, \beta, \gamma, \delta$ and the $f'_{ij}$ undetermined. Then any solution of this system defines a proper reparametrization of the ruled surface. However, the systems are generally too large and further research is needed to develop an efficient algorithmic solution to the reparametrization problem.

CHAPTER 2

# Implicitization of canal surfaces

ABSTRACT. A canal surface is an envelope of a one parameter family of spheres. In this chapter we present an efficient algorithm for computing the implicit equation of a canal surface generated by a rational family of spheres. By using Laguerre and Lie geometries, we relate the equation of the canal surface to the equation of a dual variety of a certain curve in 5-dimensional projective space. We define the $\mu$-basis for arbitrary dimension and give a simple algorithm for its computation. This is then applied to the dual variety, which allows us to represent the implicit equations of the dual variety, the canal surface and any offset to the canal surface as resultants. The results in this chapter are joint work with Severinas Zube and have been accepted for publication in [**DZ08**].

## 1. Introduction

In surface design, the user often needs to perform rounding or filleting between two intersecting surfaces. Mathematically, the surface used in making the rounding is defined as the envelope of a family of spheres which are tangent to both surfaces. This envelope of spheres centered at $c(t) \in \mathbb{R}^3$ with radius $r(t)$, where $c(t)$ and $r(t)$ are rational functions, is called a canal surface with spine curve $\mathcal{E} = \{(c(t), r(t)) \in \mathbb{R}^4 | t \in \mathbb{R}\}$. If the radius $r(t)$ is constant the surface is called a pipe surface. Moreover, if additionally we reduce the dimension (take $c(t)$ in a plane and consider circles instead of spheres) we obtain the offset to the curve. Canal surfaces are very popular in Geometric Modeling, as they can be used as a blending surface between two surfaces. For example, any two circular cones with a common inscribed sphere can be blended by a part of a Dupin cyclide bounded by two circles as it was shown by [**Pr90, Pr95**] (see Figure 1). Cyclides are envelopes of special quadratic families of spheres. For other examples of blending with canal surfaces we refer to [**Ka05**].

Partial solutions to the problem of finding the implicit equation (and degree) for canal surfaces have been given in other papers. For instance, the degree of offsets to curves is studied in [**SS05**]. In [**XFS06**], there is a degree formula for the implicit equation of a polynomial canal surface. Quadratic canal surfaces (parametric and implicit representation) have been studied in [**KZ07**].

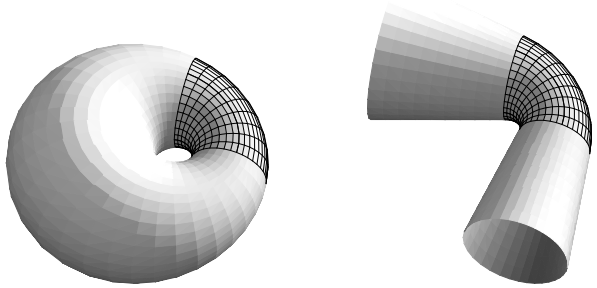


FIGURE 1. A Dupin cyclide used for blending circular cones.

Usually, the implicit equation of a canal surface is obtained after elimination of the family variable $t$ from a system of two equations $g_1(y,t) = g_2(y,t) = 0$ (where $g_1, g_2$ are quadratic in the variables $y = (y_1, y_2, y_3, y_4)$), i.e. by taking the resultant with respect to $t$. However, this resultant can have extraneous factors which are geometrically counterintuitive. In this chapter we explain how these factors appear and how we can eliminate them. Using Lie and Laguerre geometry, we relate the canal surface to a variety in higher dimension, which has similar properties as a ruled surface and for which we can apply a generalized theory of $\mu$-bases, which allows us to represent the implicit equation of the canal surface and its offsets without extraneous factors as resultants.

An interesting remark is that the $\mu$-basis is also relevant for finding a parametrization of the canal surface of minimal degree. This is studied in detail in [**Kr07**].

The chapter is organized as follows. In the next section we develop some algebraic formalism about modules with two quasi-generators. We define the $\mu$-basis for these modules, which is a generalization of the theory treated in the first chapter, and present an algorithm for its computation. In the following section, we recall some needed facts about Lie and Laguerre sphere geometry and proceed to give preliminary definitions of the geometric objects to be studied and show that they contain unwanted extraneous components. By embedding those objects in a higher dimension, we can "linearize" the problem, i.e. we place ourselves in a context in which the theory of $\mu$-bases can be used to explain and eliminate the extraneous components. We introduce the $\Gamma$-hypersurface which contains all $d$-offsets and show how the $\mu$-basis algorithm can be used to compute matrix representations of the $\Gamma$-hypersurface, the canal surface $\mathcal{C}$, and its offsets. Finally, we give some computational examples.

## 2. Modules with two quasi-generators and the $\mu$-basis.

Let $\mathbb{R}[t]$ be polynomial ring over the field of real numbers, and denote $\mathbb{R}[t]^d$ the $\mathbb{R}[t]$-module of $d$-dimensional row vectors with entries in $\mathbb{R}[t]$. Let $\mathbb{R}(t)$ be the field of rational functions in $t$. For a pair of vectors $A = (A_1, A_2, \ldots, A_d), B = (B_1, B_2, ..., B_d) \in \mathbb{R}[t]^d$ the set

$$(7) \qquad \begin{aligned} M = \langle A, B\rangle &= \{aA + bB \in \mathbb{R}[t]^d \mid a, b \in \mathbb{R}(t), A, B \in \mathbb{R}[t]^d\} \\ &\subset \mathbb{R}[t]^d \end{aligned}$$

is the $\mathbb{R}[t]$-module with two polynomial *quasi-generators* $A, B$. Here, we assume that $A, B$ are $\mathbb{R}[t]$-linearly independent, i.e. $aA + bB = 0$ with $a, b \in \mathbb{R}[t]$ if and only if $a = b = 0$.

Remark 2.1. Note that the vectors $A, B$ may not be generators of the module $M$ over $\mathbb{R}[t]$ because $a$ and $b$ in the definition (7) are from the field $\mathbb{R}(t)$ of rational functions. For example, if $A = pD$ with $p \in \mathbb{R}[t], D \in \mathbb{R}[t]^d$ and deg $p > 0$ then $A, B$ are not generators of the module $M$.

For $A = (A_1, A_2, \ldots, A_d), B = (B_1, B_2, ..., B_d) \in \mathbb{R}[t]^d$ we define the Plücker coordinate vector $A \wedge B$ as

$$A \wedge B = ([1, 2], [1, 3], ..., [d - 1, d]) \in \mathbb{R}[t]^{d(d-1)/2},$$

where $[i, j] = A_iB_j - A_jB_i$. In other words, $A \wedge B$ is the vector of 2-minors of the matrix

$$W_{A,B} = \begin{pmatrix} A_1 & A_2 & \cdots & A_d \\ B_1 & B_2 & \cdots & B_d \end{pmatrix}$$

and we denote by $\deg(A \wedge B) = \max_{i,j}\{\deg(A_iB_j - A_jB_i)\}$ the degree of the Plücker coordinate vector, i.e. the maximal degree of a 2-minor of $W_{A,B}$. Let a polynomial vector $A \in \mathbb{R}[t]^d$ be presented as

$$A = \sum_{i=0}^{n} \alpha_i t^i, \ \alpha_i \in \mathbb{R}^d, \ i = 0, ..., n; \ \alpha_n \neq 0.$$

We denote the leading vector $\alpha_n$ by $LV(A)$ and the degree of $A$ by deg $A = n$. Note that if $LV(A)$ and $LV(B)$ are linearly independent over $\mathbb{R}$ then deg $A \wedge B =$ deg $A +$ deg $B$ and $LV(A \wedge B) = LV(A) \wedge LV(B)$. We define

$$\text{deg } M = \min\{\deg(\tilde{A} \wedge \tilde{B}) \mid \quad \tilde{A}, \tilde{B} \in \mathbb{R}[t]^d \text{ such that } \langle \tilde{A}, \tilde{B}\rangle = M\}$$

to be the degree of the module $M$ with two quasi-generators.

Definition 2.2. Two quasi-generators $\tilde{A}, \tilde{B}$ of the module $M = \langle A, B\rangle$ are called a $\mu$-basis of the module $M$ if deg $M =$ deg $\tilde{A} +$ deg $\tilde{B}$.

As we always have the inequality $\deg(A \wedge B) \leq \deg A + \deg B$, this means in particular that the sum $\deg \tilde{A} + \deg \tilde{B}$ is minimal. A $\mu$-basis always exists, as we shall see at the end of the section.

REMARK 2.3. By abuse of notation, we will continue to denote parameters $t$, however in the geometric definitions that follow, they should be understood as parameters $(t : s) \in \mathbb{P}^1$ and polynomials in $\mathbb{R}[t]$ should be thought of as homogenized with respect to a new variable $s$.

Let us explain the geometric motivation behind the definition of the $\mu$-basis. We define the following subspace of $\mathbb{R}^d$ for the module $M = \langle A, B \rangle$.

$$L(M, t_0) = \{x \in \mathbb{R}^d \mid C(t_0) \cdot x = 0 \text{ for all } C \in M\}$$

where $C(t) = (C_1(t), C_2(t), \ldots, C_d(t)) \in \mathbb{R}[t]^d$, $x = (x_1, x_2, \ldots, x_d)^T$ and $C(t) \cdot x = x_1 C_1(t) + x_2 C_2(t) + \ldots + x_d C_d(t)$. We have the inequality $\dim(L(M, t_0)) \geq d - 2$, because the module $M$ has only two quasi-generators. In fact, we have $\dim(L(M, t_0)) = d - 2$ for all $t_0$, as we will see in Proposition 2.9.2. Whenever two vectors $A(t_0)$ and $B(t_0)$ are linearly independent in $\mathbb{R}^d$ then $L(M, t_0)$ is the intersection of two hyperspaces $\{x \in \mathbb{R}^d | \ A(t_0) \cdot x = 0\}$ and $\{x \in \mathbb{R}^d \mid B(t_0) \cdot x = 0\}$.

Using those subspaces, we can associate a hypersurface $\mathcal{S}_M$ in the real projective space $\mathbb{P}^{d-1} = \mathbb{P}(\mathbb{R}^d)$ with the module $M$

$$\mathcal{S}_M := \bigcup_t \mathbb{P}(L(M, t)) \subset \mathbb{P}^{d-1}. \tag{8}$$

Note that this definition and the definition of $L(M, t_0)$ depend only on the module $M$ and not on the choice of quasi-generators. It is useful to compare the hypersurface $\mathcal{S}_M$ with the hypersurface $\mathcal{S}_{A,B}$ defined as

$$\mathcal{S}_{A,B} := \bigcup_t (\{A(t) \cdot x\} \cap \{B(t) \cdot x\}) \subset \mathbb{P}^{d-1} \tag{9}$$

where $A, B$ are quasi-generators of $M$. By definition, this is the variety defined by $\operatorname{Res}_t(A(t) \cdot x, B(t) \cdot x)$ and it is clear that $\mathcal{S}_M \subset \mathcal{S}_{A,B}$. If the vectors $A(t_0), B(t_0)$ are linearly dependent, then $(\{A(t_0) \cdot x\} \cap \{B(t_0) \cdot x\}) \subset \mathbb{R}^d$ is a subspace of codimension one. Note that in this case the implicit equation $\operatorname{Res}_t(A(t) \cdot x, B(t) \cdot x)$ contains the factor $A(t_0) \cdot x$. As a matter of fact, this happens if and only if $W_{A,B}(t_0)$ has rank one, which is equivalent to saying that $t_0$ is a zero of the ideal generated by the Plücker coordinates.

In fact, we will see in Proposition 2.7 that this phenomenon does not occur for $\mu$-bases, i.e. if $\tilde{A}, \tilde{B}$ is a $\mu$-basis of the module $M$ then $\mathcal{S}_M = \mathcal{S}_{\tilde{A},\tilde{B}}$ and there are no extraneous factors as before.

REMARK 2.4. We should explain why we use the term $\mu$-basis. The above definition is a generalization of the usual definition for of the

$\mu$-basis of a rational ruled surface as in Definition 1.6. They coincide in the special case $d = 4$. $M$ is the analogue of the syzygy module (i.e. the module of moving planes following the parametrization of the ruled surface) and the subspaces $L(M, t)$, which in this case are 2-dimensional and hence define projective lines, are exactly the family of lines which constitute the ruled surface. Similarly, the case $d = 3$ corresponds at the theory of $\mu$-bases for rational curves and our definition is equivalent to the usual definition as in Definition 1.2, compare also [**CW03a**, Theorem 3, Condition 3].

However, the approach used here is actually inverse to the approach in the first chapter, where the ruled surface is defined by a parametrization and then the module of moving planes is studied, whereas here we fix a module that "looks like" such a moving plane module and then study the (generalized) ruled surface that corresponds to it. Note that by definition of the subspaces $L(M, t)$ any element $C$ of $M$ can be considered a moving plane following $\mathcal{S}_M$, in the sense that for all $x \in \mathcal{S}_M$ there is a parameter $t$ such that $C(t) \cdot x = 0$.

Note that $A \wedge B$ defines the so-called Plücker curve $\mathcal{P}$ in $\mathbb{P}^{d(d-1)/2-1}$ by

$$\begin{array}{rccc} \varphi_{\mathcal{P}} : \mathbb{P}^1 & \dashrightarrow & & \mathbb{P}^{d(d-1)/2-1} \\ t & \mapsto & ([1,2] : [1,3] : ... : [d-1,d]) \end{array}$$

where $[i, j] = A_i B_j - A_j B_i$. We will denote $k = \deg \varphi_{\mathcal{P}}$ the degree of the parametrization, which is the cardinality of the fiber of a generic point in the image of $\varphi_{\mathcal{P}}$. Note that $\varphi_{\mathcal{P}}$ and $k$ are the same for any choice of quasi-generators of $M$.

PROPOSITION 2.5. *For any pair of quasi-generators $A, B$ of $M$ we have the degree formula*

$$k \cdot \deg \mathcal{S}_M = \deg(A \wedge B) - \deg q_{A,B},$$

*where $q_{A,B} = \gcd(A \wedge B)$ and $k = deg\ \varphi_{\mathcal{P}}$. Moreover, we have* $\deg \mathcal{P} = \deg \mathcal{S}_M$.

PROOF. The proposition and the proof are similar to Lemma 1 in [**CZS01**] and to Theorem 5.3 in [**PPR98**].

The implicit degree of the hypersurface $\mathcal{S}_{A,B}$ is the number of intersections between a generic line and the hypersurface. The generic line $L(s)$ is defined by two points in the space $L(s) = H_0 + sH_1$, where $H_i = (h_{i1}, h_{i2}, ..., h_{id}), i = 0, 1$. The line $L(s)$ intersects the hyperplane $\{A(t) \cdot x\}$ if and only if $H_0 \cdot A(t) + sH_1 \cdot A(t) = 0$. Since the line $L(s)$ should intersect the hyperplane $\{B(t) \cdot x\}$ too, we see that the implicit degree is the number of intersections of two curves in the $(t, s)$ plane:

$$\begin{cases} H_0 \cdot A(t) + sH_1 \cdot A(t) & = 0 \\ H_0 \cdot B(t) + sH_1 \cdot B(t) & = 0 \end{cases}$$

Eliminating $s$ from the above equation we have

$$\begin{vmatrix} H_0 \cdot A(t) & H_1 \cdot A(t) \\ H_0 \cdot B(t) & H_1 \cdot B(t) \end{vmatrix} = (H_0 \wedge H_1) \cdot (A(t) \wedge B(t)) = 0 \tag{10}$$

where $C \cdot D$ means a standard scalar product of two vectors $C, D \in \mathbb{R}^{d(d-1)/2}$. The number of solutions of (10) is the number of intersection points of the Plücker curve with a generic hyperplane in $\mathbb{P}^{d(d-1)/2-1}$, so $\deg \mathcal{P} = \deg \mathcal{S}_M$.

Now we have seen in Theorem 1.1 that

$$k \cdot \deg \mathcal{P} = \deg(A \wedge B) - \deg q_{A,B}$$

and the proposition follows. □

We have yet to show the existence of the $\mu$-basis. To this end, we propose an algorithm for its computation, the basic idea of which is to reduce $q_{A,B} = \gcd(A \wedge B)$ to a constant using the so-called Smith form of the $2 \times d$ matrix

$$W_{A,B} = \begin{pmatrix} A_1 & A_2 & \cdots & A_d \\ B_1 & B_2 & \cdots & B_d \end{pmatrix}$$

and then render the leading vectors linearly independent by a simple degree reduction. The Smith form is a decomposition $W_{A,B} = U \cdot S \cdot V$, with unimodular $U \in \mathbb{R}[t]^{2\times 2}$, $V \in \mathbb{R}[t]^{d\times d}$, and

$$S = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & q_{A,B} & 0 & \cdots & 0 \end{pmatrix} \in \mathbb{R}[t]^{2\times d}$$

It always exists and can be computed efficiently by standard computer algebra systems.

ALGORITHM ($\mu$-basis of a module)

INPUT: Quasi-generators $A = (A_1, \ldots, A_d)$ and $B = (B_1, \ldots, B_d) \in \mathbb{R}[t]^d$ of the module $M$

(1) Set
$$W_{A,B} = \begin{pmatrix} A_1 & A_2 & \cdots & A_d \\ B_1 & B_2 & \cdots & B_d \end{pmatrix}.$$

(2) Compute a Smith form
$$W_{A,B} = U \cdot \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & q_{A,B} & 0 & \cdots & 0 \end{pmatrix} \cdot V$$
with unimodular $U \in \mathbb{R}[t]^{2\times 2}$,$V \in \mathbb{R}[t]^{d\times d}$.

(3) Set $W'$ to be the $2 \times d$-submatrix consisting of the first two rows of $V$.

(4) If the vector of leading terms (with respect to the variable $t$) of the first row is $h$ times the one of the second row, $h \in \mathbb{R}[t]$, set $W' := \begin{pmatrix} 1 & -h \\ 0 & 1 \end{pmatrix} \cdot W'$.

(5) If the vector of leading terms (with respect to the variable $t$) of the second row is $h$ times the one of the first row, $h \in \mathbb{R}[t]$, set $W' := \begin{pmatrix} 1 & 0 \\ -h & 1 \end{pmatrix} \cdot W'$.

(6) If the preceding two steps changed $W'$ go back to Step 5.

(7) Set $\tilde{A}, \tilde{B}$ to be the rows of $W'$.

OUTPUT: A $\mu$-basis $\tilde{A}, \tilde{B}$ of the module $M$

As we shall see in Section 5, the case we are interested in is the case $d = 6$, so we are dealing with very small matrices and the computations are extremely fast. Note that we actually only need the first two rows of $V$, so we could optimize the algorithm by modifying the Smith form algorithm used as not to compute the unnecessary entries of the matrices $U$ and $V$. Generally, the number of elementary matrix operations in Step 5 and 6 is very low. In the worst case, it is bounded by the maximal degree of the entries of the matrix $W'$ in Step 4 of the algorithm, since each step reduces the maximal degree in one of the rows of $W'$.

Next, we will show that the output of the above algorithm is a $\mu$-basis and that the resultant of a $\mu$-basis $\tilde{A}, \tilde{B}$ of the module $M = \langle A, B \rangle$ is an implicit equation of $\mathcal{S}_M$. In Section 5, we will use these results for a special choice of $A$ and $B$ to compute the implicit equation of a canal surface.

LEMMA 2.6. *The output of the above algorithm is a $\mu$-basis and we have $k \cdot \deg \mathcal{S}_M = \deg M$, where $k = \deg \varphi_{\mathcal{P}}$.*

PROOF. Let $\tilde{A}(t), \tilde{B}(t)$ be the output of the above algorithm. By construction it is clear that $\tilde{A}(t), \tilde{B}(t)$ are quasi-generators of $M$ and that $\tilde{q}_{A,B} = \gcd(\tilde{A} \wedge \tilde{B}) = 1$. Furthermore, we have $\deg(\tilde{A} \wedge \tilde{B}) = \deg(\tilde{A}) + \deg(\tilde{B})$, because the vectors of leading terms of $\tilde{A}(t)$ and $\tilde{B}(t)$ are linearly independent. So by Proposition 2.5 we deduce

$$\begin{aligned} k \cdot \deg \mathcal{S}_M &= \deg(\tilde{A} \wedge \tilde{B}) - \deg(\tilde{q}) \\ &= \deg(\tilde{A} \wedge \tilde{B}) \\ &= \deg(\tilde{A}) + \deg(\tilde{B}) \end{aligned}$$

Moreover, by definition we have $\deg M \leq \deg(\tilde{A} \wedge \tilde{B})$ and if $A, B$ are quasi-generators such that $\deg(A \wedge B)$ is minimal, the degree formula

gives $\deg(\tilde{A} \wedge \tilde{B}) = \deg(A \wedge B) - \deg(q) \leq \deg M$, which shows that $k \cdot \deg \mathcal{S}_M = \deg M$, and as a consequence that $\tilde{A}(t), \tilde{B}(t)$ is indeed a $\mu$-basis. □

PROPOSITION 2.7. *Let $x = (x_1, x_2, \ldots, x_d)^T$ be variables and $\tilde{A}(t), \tilde{B}(t)$ a $\mu$-basis of $M$. Then*

$$\operatorname{Res}_t(\tilde{A}(t) \cdot x, \tilde{B}(t) \cdot x) = F_{\mathcal{S}_M}^k$$

*where $F_{\mathcal{S}_M}$ is the implicit equation of the hypersurface $\mathcal{S}_M$. In particular, any matrix of the above resultant (e.g. Sylvester or Bézout) is a square representation matrix of $\mathcal{S}_M$.*

PROOF. First, we will show in the same way as in Theorem 1.11 that $\operatorname{Res}_t(\tilde{A}(t) \cdot x, \tilde{B}(t) \cdot x)$ is geometrically irreducible, i.e. the power of an irreducible polynomial. As we shall see in Proposition 2.9, the intersection of the hyperplanes $\{\tilde{A}(t) \cdot x\}$ and $\{\tilde{B}(t) \cdot x\}$ is of codimension 2 for any parameter $t \in \mathbb{P}^1$. So the incidence variety

$$\mathcal{W} = \{(t, x) \in \mathbb{P}^1 \times \mathbb{P}^{d-1} | \tilde{A}(t) \cdot x = \tilde{B}(t) \cdot x = 0\} \subset \mathbb{P}^1 \times \mathbb{P}^{d-1}$$

is a vector bundle over $\mathbb{P}^1$ and hence irreducible. So the projection on $\mathbb{P}^{d-1}$ is irreducible as well and its equation, which is by definition the hypersurface defined by $\operatorname{Res}_t(\tilde{A}(t) \cdot x, \tilde{B}(t) \cdot x)$, is a power of an irreducible polynomial.

As we have remarked earlier, the resultant of two quasi-generators is always a multiple of the implicit equation of $\mathcal{S}_M$, so $\operatorname{Res}_t(\tilde{A}(t) \cdot x, \tilde{B}(t) \cdot x)$ is a power of $F_{\mathcal{S}_M}$.

But using the degree property above we see

$$\deg(\operatorname{Res}_t(\tilde{A}(t) \cdot x, \tilde{B}(t) \cdot x)) = \deg(\tilde{A}) + \deg(\tilde{B}) = k \cdot \deg \mathcal{S}_M$$

which implies that $\operatorname{Res}_t(\tilde{A}(t) \cdot x, \tilde{B}(t) \cdot x)$ equals $F_{\mathcal{S}_M}^k$. □

REMARK 2.8. It is known that the Plücker curve $\mathcal{P}$ can be properly reparametrized, i.e. there exists a rational function $h$ of degree $k$ such that $A \wedge B = C \circ h$, where $C$ is a proper parametrization of $\mathcal{P}$. It is tempting to use this proper reparametrization in order to represent the implicit equation $F_{\mathcal{S}_M}$ of $\mathcal{S}_M$ directly as a resultant as in the proof of Theorem 1.4. However, $h$ does not necessarily factorize $A$ and $B$, i.e. it is not sure that there exist $A'$ and $B'$ with $A = A' \circ h$ and $B = B' \circ h$, which would be needed to do this.

In the following we present some properties of $\mu$-bases. Note that the properties in Propositions 2.9, 2.10 are similar to [**CW03a**] Theorems 1,3. However, we give different proofs by deducing them from the degree formula and Lemma 2.6.

PROPOSITION 2.9. *Let $M = \langle A, B \rangle$ and let $\tilde{A}, \tilde{B}$ be a $\mu$-basis of the module $M$. Then the following properties hold:*
*1. The vectors $LV(\tilde{A}), LV(\tilde{B})$ are linearly independent.*

*2.* $\tilde{A}(t_0), \tilde{B}(t_0)$ *are linearly independent over* $\mathbb{C}$ *for any parameter value* $t_0 \in \mathbb{C}$.

PROOF. 1. If $LV(\tilde{A}), LV(\tilde{B})$ were linearly dependent, this would imply that $k \cdot \deg \mathcal{S}_M = \deg(\tilde{A} \wedge \tilde{B}) - \deg(q_{\tilde{A},\tilde{B}}) < \deg(\tilde{A}) + \deg(\tilde{B}) = \deg M$ which is a contradiction to Lemma 2.6.
2. Suppose that $\tilde{A}(t_0), \tilde{B}(t_0)$ are linearly dependent for some $t_0 \in \mathbb{C}$. This is equivalent to saying that the matrix $W_{\tilde{A},\tilde{B}}$ is not of full rank, which means that all 2-minors vanish. So $t_0$ is a root of $q_{\tilde{A},\tilde{B}}$ and as above we deduce $k \cdot \deg \mathcal{S}_M = \deg(\tilde{A} \wedge \tilde{B}) - \deg(q_{\tilde{A},\tilde{B}}) < \deg(\tilde{A}) + \deg(\tilde{B}) = \deg M$ which is again a contradiction to Lemma 2.6. □

PROPOSITION 2.10. *Let* $M = \langle \tilde{A}, \tilde{B} \rangle$ *and assume that* $\tilde{A}, \tilde{B}$ *satisfy conditions 1,2 from Proposition 2.9. Then any element* $D \in M$ *has the following expression:* $D = h_1\tilde{A} + h_2\tilde{B}$ *for some* $h_1, h_2 \in \mathbb{R}[t]$, *i.e.* $\tilde{A}, \tilde{B}$ *are generators of the module* $M$ *over the polynomial ring* $\mathbb{R}[t]$. *Moreover, the pair* $\tilde{A}, \tilde{B}$ *is a* $\mu$*-basis of the module* $M$.

PROOF. Let $D \in M$, it can be expressed as

$$D = \frac{a}{b}\tilde{A} + \frac{c}{d}\tilde{B}$$

with $a, b, c, d \in \mathbb{R}[t]$ and co-prime numerators and denominators in the rational functions $\frac{a}{b}$ and $\frac{c}{d}$. Furthermore, we may assume that $\gcd(a, c) = 1$, because if $\frac{D}{\gcd(a,c)}$ is a linear combination of $\tilde{A}, \tilde{B}$, then so is $D$. Multiplying both sides of the above equation with $bd$ we obtain $bdD = ad\tilde{A} + bc\tilde{B}$ or equivalently $b(dD - c\tilde{B}) = ad\tilde{A}$ and since $b$ divides neither $a$ nor $\tilde{A}$ (if it divided $\tilde{A}$, for any root $t_0$ of $b$ and any constant $\alpha$ we would deduce the relation $0 = \alpha\tilde{A}(t_0) + 0 \cdot \tilde{B}(t_0)$, which contradicts property 2 in Proposition 2.9), one concludes that $b$ divides $d$ and by a symmetric argument that $d$ divides $b$, so we may assume $b = d$. So we have

$$bD = a\tilde{A} + c\tilde{B}$$

and plugging a root $t_0$ of $b$ into the equation, we would obtain a non-trivial linear relation between $\tilde{A}$ and $\tilde{B}$, again a contradiction to Proposition 2.9. This implies that $b$ and $d$ are constant, which shows that any $D \in M$ can be expressed as linear combination of $\tilde{A}$ and $\tilde{B}$ over $\mathbb{R}[t]$. In other words: $\tilde{A}$ and $\tilde{B}$ are not only quasi-generators of $M$, but actually generators in the usual sense, i.e. over $\mathbb{R}[t]$.

Suppose that $\deg\tilde{A} \leq \deg\tilde{B}$ and let $M = \langle P_1, P_2 \rangle$. Then we proved that $P_i = h_{i1}\tilde{A} + h_{i2}\tilde{B}, i = 1, 2$ for some polynomials $h_{ij} \in \mathbb{R}[t]$. Since $LV(\tilde{A}), LV(\tilde{B})$ are linearly independent $LV(h_{i1}\tilde{A})$ and $LV(h_{i2}\tilde{B}), i = 1, 2$ do not cancel each other. Therefore, $\deg P_1 \geq \deg \tilde{B}$ (if $h_{12} \neq 0$) or $\deg P_2 \geq \deg \tilde{B}$ (if $h_{22} \neq 0$). Also $\deg P_1 \geq \deg \tilde{A}$ and $\deg P_2 \geq \deg \tilde{A}$.

So, we see that $\deg P_1 + \deg P_2 \geq \deg \tilde{A} + \deg \tilde{B}$, i.e. a pair $\tilde{A}, \tilde{B}$ is a $\mu$-basis of the module $M$. □

## 3. Elements of Lie and Laguerre sphere geometry

Here we shortly recall the elements of Lie and Laguerre Sphere Geometry (cf. [**Ce92, PP98, KM00**]). We start from the construction of Lie's geometry of oriented spheres and planes in $\mathbb{R}^3$. Let $\mathbf{p} \in \mathbb{R}^3$, $r \in \mathbb{R}$. The oriented sphere $S_{\mathbf{p},r}$ in $\mathbb{R}^3$ is the set

$$S_{\mathbf{p},r} = \{\mathbf{v} \in \mathbb{R}^3 | (\mathbf{v} - \mathbf{p}) \cdot (\mathbf{v} - \mathbf{p}) = r^2\},$$

where by $\mathbf{v} \cdot \mathbf{w}$ we denote the standard positive definite scalar product in $\mathbb{R}^3$. The orientation is determined by the sign of $r$: the normals are pointing outwards if $r > 0$. If $r = 0$ then $S_{\mathbf{p},0} = \{\mathbf{p}\}$ is a point. Let $\mathbf{n} \in \mathbb{R}^3$ with $\mathbf{n} \cdot \mathbf{n} = 1$ and $h \in \mathbb{R}$. The oriented plane $P_{\mathbf{n},h}$ in $\mathbb{R}^3$ is the set

$$P_{\mathbf{n},h} = \{\mathbf{v} \in \mathbb{R}^3 | \mathbf{v} \cdot \mathbf{n} = h\}.$$

The *Lie scalar* product with signature $(4, 2)$ in $\mathbb{R}^6$ is defined by the formula

$$[x, z] = \frac{-x_1 z_2 - x_2 z_1}{2} + x_3 z_3 + x_4 z_4 + x_5 z_5 - x_6 z_6.$$

for $x = (x_1, \ldots, x_6)$ and $z = (z_1, \ldots, z_6)$. In matrix notation we have

$$[x, z] = xCz^T, \quad \text{where } xC = (-x_2/2, -x_1/2, x_3, x_4, x_5, -x_6). \tag{11}$$

Denote $\hat{y} = (u : y_0 : y_1 : y_2 : y_3 : y_4) \in \mathbb{P}(\mathbb{R}^6) = \mathbb{P}^5$ and define the quadric

$$\mathcal{Q} = \{\hat{y} \in \mathbb{P}^5 \mid [\hat{y}, \hat{y}] = -uy_0 + y_1^2 + y_2^2 + y_3^2 - y_4^2 = 0\} \tag{12}$$

where $[.,.]$ is the obvious extension of the Lie scalar product to $\mathbb{P}^5$. $\mathcal{Q}$ is called *Lie quadric*.

We represent an oriented sphere $S_{\mathbf{p},r}$ (or an oriented plane $P_{\mathbf{n},h}$) as a point $Lie(S_{\mathbf{p},r})$ (resp. $Lie(P_{\mathbf{n},h})$) on the Lie quadric:

$$\begin{aligned} Lie(S_{\mathbf{p},r}) &= (2(\mathbf{p} \cdot \mathbf{p} - r^2), 2, 2\mathbf{p}, 2r) \in \mathcal{Q}, \quad \mathbf{p} \in \mathbb{R}^3, r \in \mathbb{R}, \\ Lie(P_{\mathbf{n},h}) &= (2h, 0, \mathbf{n}, 1) \in \mathcal{Q}, \quad \mathbf{n} \in \mathbb{R}^3,\ h \in \mathbb{R}. \end{aligned}$$

It is easy to see that we have determined a bijective correspondence between the set of points on the Lie quadric $\mathcal{Q}$ and the set of all oriented spheres/planes in $\mathbb{R}^3$. Here we assume that a point $q = (1 : 0 : 0 : 0 : 0 : 0) \in \mathcal{Q}$ on the Lie quadric $\mathcal{Q}$ corresponds to an infinity, i.e. to a point in the compactification of $\mathbb{R}^3$. We say that $q = (1 : 0 : 0 : 0 : 0 : 0)$ is the improper point on the Lie quadric. Notice that oriented planes in $\mathbb{R}^3$ correspond to points $\mathcal{Q} \cap T_q$, where $T_q = \{\hat{y} = (u : y_0 : y_1 : y_2 : y_3 : y_4) \in \mathbb{P}^5 | y_0 = 0\}$ is a tangent hyperplane to the Lie quadric at the improper point $q$.

Two oriented spheres $S_{\mathbf{p}_1,r_1}, S_{\mathbf{p}_2,r_2}$ are in *oriented contact* if they are tangent and have the same orientation at the point of contact. The analytic condition for oriented contact is

$$\|\mathbf{p}_1 - \mathbf{p}_2\| = |r_1 - r_2|,$$

where $\|\mathbf{p}_1 - \mathbf{p}_2\|$ denotes the usual distance between two points in the Euclidean space $\mathbb{R}^3$. One can check directly that the analytical condition of oriented contact on the Lie quadric is equivalent to the equation

$$[Lie(S_{\mathbf{p}_1,r_1}), Lie(S_{\mathbf{p}_2,r_2})] = 0.$$

It is known that the Lie quadric contains projective lines but no linear subspaces of higher dimension (Chapter 1, Corollary 5.2 in [**Ce92**]). Moreover, the line in $\mathbb{P}^5$ determined by two points $k_1, k_2$ of $\mathcal{Q}$ lies on $\mathcal{Q}$ if and only $[k_1, k_2] = 0$, i.e. the corresponding spheres to $k_1, k_2$ are in an oriented contact (Chapter 1, Theorem 1.5.4 in [**Ce92**]). The points on a line on $\mathcal{Q}$ form so called *parabolic pencil* of spheres. All spheres which correspond to a line on $\mathcal{Q}$ are precisely the set of all spheres in an oriented contact.

Remark 2.11. Here we use a slightly different coordinate system in Lie Geometry than in the book [**Ce92**]. The scalar product as in [**Ce92**] may be obtained applying the following transformation:
$x_1' = (x_1 + x_2)/2, x_2' = (x_2 - x_1)/2, x_3' = x_3, x_4' = x_4, x_5' = x_5, x_6' = x_6$.

We show now that the set of points $\hat{y}$ in $\mathcal{Q}$ with $y_0 \neq 0$ is naturally diffeomorphic to the affine space $\mathbb{R}^4$. This diffeomorphism is defined by the map

$$\begin{array}{rccc} \phi: & \mathcal{Q} \setminus T_q & \to & \mathbb{R}^4, \\ & (u : y_0 : y_1 : y_2 : y_3 : y_4) & \mapsto & \left(\frac{y_1}{y_0}, \frac{y_2}{y_0}, \frac{y_3}{y_0}, \frac{y_4}{y_0}\right), \end{array}$$

where $T_q = \{\hat{y} = (u : y_0 : y_1 : y_2 : y_3 : y_4) \in \mathbb{P}^5 \mid y_0 = 0\}$ as before, i.e. the tangent hyperplane to the Lie quadric $\mathcal{Q}$ at the improper point $q = (1 : 0 : 0 : 0 : 0 : 0)$. Let $v = (v_1, v_2, v_3, v_4), w = (w_1, w_2, w_3, w_4) \in \mathbb{R}^4$ and denote by

$$\langle v, w\rangle = v_1w_1 + v_2w_2 + v_3w_3 - v_4w_4$$

the Lorentz scalar product on $\mathbb{R}^4$, which can be seen as the restriction of the Lie scalar product $[.,.]$ to $\mathbb{R}^4$. The affine space $\mathbb{R}^4$ with the Lorentz scalar product is called the Lorentz space and denoted by $\mathbb{R}^4_1$.

Let $y = (y_1, y_2, y_3, y_4) \in \mathbb{R}^4$. One can check that inverse map of $\phi$ is given by the formula:

$$\phi^{-1}(y) = (\langle y, y\rangle, 1, y) \in \mathcal{Q} \setminus T_q$$

Notice, that $\phi(Lie(S_{\mathbf{p},r})) = (\mathbf{p}, r)$, i.e. the sphere $S_{\mathbf{p},r} \in \mathbb{R}^3$ corresponds to a point $(\mathbf{p}, r) \in \mathbb{R}^4_1$. The map $\phi$ can be extended to a linear

projection $\Phi$ from $\mathcal{Q} \setminus \{q\}$ to $\mathbb{P}^4$ defined as

$$\begin{array}{lccc} \Phi: & \mathcal{Q} \setminus \{q\} & \to & \mathbb{P}^4 \\ (u : y_0 : y_1 : y_2 : y_3 : y_4) & \mapsto & (y_0 : y_1 : y_2 : y_3 : y_4) \end{array}$$

The points of $\mathcal{Q} \cap T_q$ can be represented as $Lie(P_{\mathbf{n},h}) = (2h, 0, \mathbf{n}, 1)$ and these points correspond to planes in $\mathbb{R}^3$. Note that

$$\Phi(Lie(P_{\mathbf{n},h})) = (0, \mathbf{n}, 1) \in \Omega = \{y_0 = 0, y_1^2 + y_2^2 + y_3^2 - y_4^2 = 0\}$$

are infinite points to the natural extension of $\mathbb{R}^4$ to $\mathbb{P}^4$ which correspond to a pencil of parallel planes in $\mathbb{R}^3$. The quadric $\Omega$ is called *absolute quadric*. The preimage of the map $\Phi$ has the following form

$$\Phi^{-1}(\overline{y}) = (\langle y, y \rangle : y_0^2 : y_0 y_1 : y_0 y_2 : y_0 y_3 : y_0 y_4) \in \mathcal{Q} \setminus \{q\} \tag{13}$$

where $\overline{y} = (y_0 : y_1 : y_2 : y_3 : y_4) \in \mathbb{P}^4$ and $y = (y_1, y_2, y_3, y_4)$ as before. A direct computation shows that for $v, w \in \mathbb{R}^4$

$$-2[\phi^{-1}(v), \phi^{-1}(w)] = \langle v - w, v - w \rangle \tag{14}$$

The formula shows that two oriented spheres defined by $v$, $w$ (i.e. spheres $S_{(v_1,v_2,v_3),v_4}$ and $S_{(w_1,w_2,w_3),w_4}$) are in oriented contact if and only if $\langle v - w, v - w \rangle = 0$.

Let us define two maps: an embedding $i_d : \mathbb{R}^3 \to \mathbb{R}^4, i_d(\mathbf{p}) = (\mathbf{p}, d), d \in \mathbb{R}$ and a projection $\pi : \mathbb{R}^4 \to \mathbb{R}^3, \pi(\mathbf{p}, r) = \mathbf{p}$, where $r \in \mathbb{R}$. We will treat points $i_0(\mathbb{R}^3)$ as spheres with zero radius and identify them with $\mathbb{R}^3$. All interrelations between the spaces introduced above can be described in the following diagram

$$\begin{array}{ccccccc} & & & \mathcal{Q} \setminus T_q & \subset & \mathcal{Q} \setminus \{q\} & \subset & \mathbb{P}^5 \\ & & & \downarrow \phi & & \downarrow \Phi & & \\ \mathbb{R}^3 & \xrightarrow{i_d} & \mathbb{R}^4 & & \subset & \mathbb{P}^4 & & \\ \| & & \downarrow \pi & & & & & \\ \mathbb{R}^3 & = & \mathbb{R}^3 & & & & & \end{array} \tag{15}$$

Definition 2.12. For an oriented surface (curve or point) $\mathcal{M} \subset \mathbb{R}^3$ define an *isotropic hypersurface* $\mathcal{G}(\mathcal{M}) \subset \mathbb{P}^4$ as the union of all points in $\mathbb{R}^4$ which correspond to oriented tangent spheres of $\mathcal{M}$. Let $\mathcal{G}_d(\mathcal{M}) = \mathcal{G}(\mathcal{M}) \cap \{y_4 = dy_0\}$ be a variety which corresponds to tangent spheres with radius $d$ of $\mathcal{M}$. The set $\mathrm{Env}_d(\mathcal{M}) = \pi(\mathcal{G}_d(\mathcal{M})|_{\mathbb{R}^4}) \subset \mathbb{R}^3$ are centers of spheres with radius $d$ tangent to $\mathcal{M}$. The set $\mathrm{Env}_d(\mathcal{M})$ is called $d$-envelope of the variety $\mathcal{M}$. Since $\mathcal{G}(\mathcal{M}) = \bigcup_d \mathcal{G}_d(\mathcal{M})$ we can treat the isotropic hypersurface $\mathcal{G}(\mathcal{M})$ as the union of all $d$-envelope to the variety $\mathcal{M}$.

If $y, a \in \mathbb{R}^4,\ a_0, y_0 \in \mathbb{R}$, we define a function

$$\begin{aligned} g((a_0 : a), (y_0 : y)) &= \langle ay_0 - a_0 y, ay_0 - a_0 y\rangle \\ &= y_0^2 a_0^2 \left\langle \frac{a}{a_0} - \frac{y}{y_0}, \frac{a}{a_0} - \frac{y}{y_0} \right\rangle \\ &= y_0^2\langle a, a\rangle - 2a_0 y_0 \langle a, y\rangle + a_0^2\langle y, y\rangle. \end{aligned} \tag{16}$$

Let $(y_0 : y)$ be such that $g((a_0 : a), (y_0 : y)) = 0$. By the formula (14) we see that spheres $S_{\left(\frac{a_1}{a_0}, \frac{a_2}{a_0}, \frac{a_3}{a_0}\right), \frac{a_4}{a_0}}$ and $S_{\left(\frac{y_1}{y_0}, \frac{y_2}{y_0}, \frac{y_3}{y_0}\right), \frac{y_4}{y_0}}$ are in oriented contact. Therefore, in the same manner as previously, we define the isotropic hypersurface $\mathcal{G}((a_0 : a))$ as follows

$$\mathcal{G}((a_0 : a)) = \{(y_0, y) \in \mathbb{P}^4 \mid g((a_0 : a), (y_0 : y)) = 0\} \subset \mathbb{P}^4.$$

In fact, $\mathcal{G}((a_0 : a))$ is a quadratic cone with a singular point at a vertex $(a_0 : a) \in \mathbb{P}^4$ and may be viewed as the set of all spheres which touches the fixed sphere $S_{\left(\frac{a_1}{a_0}, \frac{a_2}{a_0}, \frac{a_3}{a_0}\right), \frac{a_4}{a_0}}$. After the restriction to the linear subspace $y_4 = dy_0$ this hypersurface consists of all spheres with radius $d$ which are in oriented contact with the sphere $S_{\left(\frac{a_1}{a_0}, \frac{a_2}{a_0}, \frac{a_3}{a_0}\right), \frac{a_4}{a_0}}$ which we denote as $\mathcal{G}_d((a_0 : a)) = \mathcal{G}((a_0 : a)) \cap \{y_4 = dy_0\}$. We notice that $\mathcal{G}_d((a_0 : a))|_{y_0=1}$ is defined by the equation $(a_1 - a_0 y_1)^2 + (a_2 - a_0 y_2)^2 + (a_3 - a_0 y_3)^2 = (a_4 - a_0 d)^2$, i.e.

$$\begin{aligned} \pi(\mathcal{G}_d((a_0 : a))|_{\mathbb{R}^4}) &= S_{\left(\frac{a_1}{a_0}, \frac{a_2}{a_0}, \frac{a_3}{a_0}\right), \frac{a_4 - a_0 d}{a_0}} = \mathrm{Env}_{-d}\left(S_{\left(\frac{a_1}{a_0}, \frac{a_2}{a_0}, \frac{a_3}{a_0}\right), \frac{a_4}{a_0}}\right) \\ \text{and} \quad \mathcal{G}_d((a_0 : a))|_{\mathbb{R}^4} &= i_d\left(S_{\left(\frac{a_1}{a_0}, \frac{a_2}{a_0}, \frac{a_3}{a_0}\right), \frac{a_4 - a_0 d}{a_0}}\right) \end{aligned}$$

Therefore, in this case, the isotropic hypersurface $\mathcal{G}((a_0 : a))$ may be treated as a union all envelopes to the sphere $S_{\left(\frac{a_1}{a_0}, \frac{a_2}{a_0}, \frac{a_3}{a_0}\right), \frac{a_4}{a_0}}$ . In the next section we generalize the definition of the isotropic hypersurface $\mathcal{G}(\mathcal{M})$ for a curve $\mathcal{M}$ in $\mathbb{R}^4$ (or $\mathbb{P}^4$).

All lines in $\mathbb{R}^4_1$ with directional vectors $v$ can be classified into three types depending on the sign of $\langle v, v\rangle$: $(+)$-lines, $(0)$-lines (also called *isotropic* lines), and $(-)$-lines.

## 4. The isotropic hypersurface and $d$-envelopes

In this section, we will see that the definition of the canal surface is not obvious and we will introduce some geometrical objects related to it. A canal surface is given by a so-called *spine curve* $\mathcal{E}$, which is the closed image (with respect to the Zariski topology) of a rational map

$$\begin{array}{ccc} \mathbb{R} & \dashrightarrow & \mathbb{R}^4 \\ t & \mapsto & \left(\frac{e_1(t)}{e_0(t)}, \frac{e_2(t)}{e_0(t)}, \frac{e_3(t)}{e_0(t)}, \frac{e_4(t)}{e_0(t)}\right) \end{array}$$

with polynomials $e_0, \ldots, e_4 \in \mathbb{R}[t]$ such that $n = \max_{i=0,..,4}\{\deg(e_i)\}$. For abbreviation, we usually skip the variable $t$ in the notations. The

spine curve describes a family of spheres $\{S_{\left(\frac{e_1(t)}{e_0(t)},\frac{e_2(t)}{e_0(t)},\frac{e_3(t)}{e_0(t)}\right),\frac{e_4(t)}{e_0(t)}} \mid t \in \mathbb{R}\}$ whose centers are given by the first three coordinates $\left(\frac{e_1(t)}{e_0(t)}, \frac{e_2(t)}{e_0(t)}, \frac{e_3(t)}{e_0(t)}\right)$ and whose radii are given by the last coordinate $\frac{e_4(t)}{e_0(t)}$. Intuitively, the canal surface is the envelope of this family of spheres, but there are some subtleties to consider before we can make a precise definition.

We can also consider the spine curve as a projective curve $\overline{\mathcal{E}}$ given as the closed image of a parametrization

$$\begin{array}{ccc} \mathbb{P}^1 & \dashrightarrow & \mathbb{P}^4 \\ t & \mapsto & (e_0(t) : e_1(t) : e_2(t) : e_3(t) : e_4(t)) \end{array}$$

with the non-restrictive condition $\gcd(e_0, \ldots, e_4) = 1$, which means that there are no base-points (i.e. parameters for which the map is not well-defined).

Note that in this case the polynomials $e_i$ are actually to be considered as homogenized to the same degree $n$ with respect to a new variable $s$. As there is a one-to-one correspondence between the univariate polynomials of a certain degree and their homogeneous counterparts, we will keep the notation from above and distinguish between the affine and projective case only where it is necessary to avoid confusion. In the following we use the notations

$$\begin{array}{ll} e = (e_1, e_2, e_3, e_4), & y = (y_1, y_2, y_3, y_4), \\ \overline{e} = (e_0 : e_1 : e_2 : e_3 : e_4), & \overline{y} = (y_0 : y_1 : y_2 : y_3 : y_4). \end{array}$$

We first proceed to define a hypersurface in $\mathbb{P}^4$ which is closely related to the canal surface.

Definition 2.13. The *isotropic hypersurface* $\mathcal{G}(\overline{\mathcal{E}}) = \{\overline{y} \mid G(\overline{y}) = 0\} \subset \mathbb{P}^4$ associated with the (projective) spine curve $\overline{\mathcal{E}}$ is the variety in $\mathbb{P}^4$ defined by the polynomial $G(\overline{y}) = \operatorname{Res}_t(g_1, g_2)$ where

$$\begin{aligned} g_1(\overline{y}, t) &= (e_0y_1 - e_1y_0)^2 + (e_0y_2 - e_2y_0)^2 \\ &\quad +(e_0y_3 - e_3y_0)^2 - (e_0y_4 - e_4y_0)^2 \\ &= \langle e_0y - y_0e, e_0y - y_0e\rangle \\ &= e_0^2\langle y, y\rangle - 2\langle e_0e, y_0y\rangle + y_0^2\langle e, e\rangle = g(\overline{e}, \overline{y}) \\ g_2(\overline{y}, t) &= \frac{\partial g_1(\overline{y}, t)}{\partial t} = 2(e_0e_0'\langle y, y\rangle - \langle (e_0e)', y_0y\rangle + y_0^2\langle e', e\rangle) \end{aligned}$$

So, we define $\mathcal{G}(\overline{\mathcal{E}})$ as the envelope of the family of isotropic hypersurfaces $\mathcal{G}(\overline{e}) = \mathcal{G}((e_0(t) : e(t))$.

In the previous section we showed that $\mathcal{G}_d(\overline{e})|_{\mathbb{R}^4} = \operatorname{Env}_{-d}\left(S_{\left(\frac{e_1}{e_0},\frac{e_2}{e_0},\frac{e_3}{e_0}\right),\frac{e_4}{e_0}}\right)$. This interpretation leads to the following definition.

DEFINITION 2.14. The *$d$-envelope* associated with the (projective) spine curve $\overline{\mathcal{E}}$ is defined as the hypersurface $\mathrm{Env}_d(\overline{\mathcal{E}}) \subset \mathbb{P}^3$ given by the implicit equation

$$G_d(y_0, y_1, y_2, y_3) = \mathrm{Res}_t(g_1|_{y_4=-dy_0}, g_2|_{y_4=-dy_0}) = \mathrm{Res}_t(g_1, g_2)|_{y_4=-dy_0},$$

i.e. the equation obtained by replacing $y_4$ in $G(\overline{y})$ by $-dy_0$, where $d \in \mathbb{R}$. The *affine envelope* $\mathrm{Env}_d(\mathcal{E})$ at distance $d$ is the restriction of $\mathrm{Env}_d(\overline{\mathcal{E}})$ to the affine space $\mathbb{R}^3$, defined by the equation $G_d|_{y_0=1} = \mathrm{Res}_t(g_1, g_2)|_{y_4=-dy_0, y_0=1}$, i.e. by setting $y_0 = 1$.

So $\mathcal{G}(\overline{\mathcal{E}})$ contains all offsets associated with the spine curve $\overline{\mathcal{E}}$. Indeed, the surface

$$\mathrm{Env}_d(\overline{\mathcal{E}}) = \mathcal{G}(\overline{\mathcal{E}}) \cap \{y_4 = -dy_0\}$$

is a hyperplane section of $\mathcal{G}(\overline{\mathcal{E}})$, which can be interpreted as a parametrization of all offsets (with respect to the parameter $y_4$).

The special case $d = 0$ is particularly important. For the real part of $\mathrm{Env}_0(\mathcal{E})$ to be non-empty, one has to suppose that $\mathcal{E}$ has tangent $(+)$-lines almost everywhere, or equivalently that $\langle e, e\rangle > 0$ almost everywhere. $\mathrm{Env}_0(\mathcal{E})$ is the envelope of the family of spheres in $\mathbb{R}^3$ given by the spine curve $\mathcal{E}$ and $\mathrm{Env}_d(\mathcal{E})$ is the envelope of the same family of spheres with radii augmented by $d$. For instance, circular cylinders or circular cones (call them just *cones*) are envelopes $\mathrm{Env}_0(\mathcal{L})$ of $(+)$-lines $\mathcal{L}$ and vice versa. In the literature, the canal surface $\mathcal{C}$ is usually defined as this envelope $\mathrm{Env}_0(\mathcal{E})$. However, we will show in an example that these envelopes can contain "unwanted" extraneous factors, which are geometrically counterintuitive.

EXAMPLE 2.15. Consider the spine curve $\mathcal{E}$ given by

$$\left(\frac{e_1(t)}{e_0(t)}, \frac{e_2(t)}{e_0(t)}, \frac{e_3(t)}{e_0(t)}, \frac{e_4(t)}{e_0(t)}\right) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}, 0, \frac{1}{2}\right).$$

The first three coordinates describe a circle in the plane and moving spheres of constant radius along this curve, so intuitively the envelope should be a torus $\mathcal{T}$. But it turns out that the implicit equation of $\mathrm{Env}_0(\mathcal{E})$ is up to a constant computed as

$$G_0 = \mathrm{Res}_t(g_1, g_2)|_{y_4=0, y_0=1} = (y_1^2 + y_2^2)^2(4y_1^2 + 4y_2^2 + 4y_3^2 + 8y_1 + 3)F_{\mathcal{T}}$$

where $F_{\mathcal{T}}$ is indeed the equation of the torus. To understand where the other factors come from, consider the following: For a given parameter $t$, the equations $g_1$ and $g_2$ define spheres $\mathcal{S}_1(t)$ and $\mathcal{S}_2(t)$ in $\mathbb{R}^3$ and

$$\mathrm{Env}_0(\mathcal{E}) = \bigcup_t \mathcal{S}_1(t) \cap \mathcal{S}_2(t)$$

of the intersections of these spheres (actually this is nothing else than the geometric definition of the resultant). Now, while for almost all $t$

this intersection is a transversal circle on the torus (often called characteristic circle in the literature), it can happen that the spheres degenerate either to planes or to the whole space. In our example, for the parameters $t = i$ and $t = -i$ we have $g_1(i) = g_1(-i) = 0$, $g_2(i) = -iy_1 + y_2$ and $g_2(-i) = iy_1 + y_2$, so the intersection in those parameters actually degenerates to (complex) planes which correspond to the factor $(-iy_1 + y_2)(iy_1 + y_2) = y_1^2 + y_2^2$. In the parameter $t = \infty$, both $g_1$ and $g_2$ define the same sphere whose equation $4y_1^2 + 4y_2^2 + 4y_3^2 + 8y_1 + 3$ is the other extraneous factor. This kind of phenomenon can also happen for real parameter values, but it is interesting to remark that even though we consider a real parametrization, non-real parameters can interfere with the envelope, because the resultant "knows" about them.

This example shows that $\mathrm{Env}_0(\mathcal{E})$ is not a suitable definition for the canal surface $\mathcal{C}$ and we will later develop one that avoids the kind of extraneous components we have observed.

Remark 2.16. It is tempting to define $\mathrm{Env}_0(\mathcal{E})$ in affine space as the resultant

$$\begin{aligned}
\check{G}_0(y_1, y_2, y_3) &= \mathrm{Res}_t(\check{g}_1(y_1, y_2, y_3, t), \check{g}_2(y_1, y_2, y_3, t)), \text{ where} \\
\check{g}_1 &= e_0^2 \check{f}_1, \qquad \check{g}_2 = e_0^3 \check{f}_2, \\
\check{f}_1 &= \left(y_1 - \frac{e_1}{e_0}\right)^2 + \left(y_2 - \frac{e_2}{e_0}\right)^2 + \left(y_3 - \frac{e_3}{e_0}\right)^2 - \left(\frac{e_4}{e_0}\right)^2, \\
\check{f}_2 &= \frac{\partial \hat{f}_1}{\partial t}
\end{aligned}$$

or in other words by deriving the affine equation of the sphere after the substitutions $y_4 = 0, y_0 = 1$ and homogenizing afterwards. Note that in this case $\check{f}_2$ and $\check{g}_2$ are linear in $y_1, y_2, y_3$. Let $\tilde{f}_1 = g_1|_{y_4=0,y_0=1}$ and $\tilde{f}_2 = g_2|_{y_4=0,y_0=1}$. An easy computation shows that we have the following equalities

$$\check{g}_1 = \tilde{f}_1, \quad \check{g}_2 = e_0 \tilde{f}_2 - 2e_0' \tilde{f}_1.$$

Therefore, by standard properties of the resultant we have

$$\begin{aligned}
\mathrm{Res}_t(\check{g}_1, \check{g}_2) &= \mathrm{Res}_t(\tilde{f}_1, e_0 \tilde{f}_2 - 2e_0' \tilde{f}_1) \\
&= \mathrm{Res}_t(\tilde{f}_1, e_0 \tilde{f}_2) \\
&= \mathrm{Res}_t(\tilde{f}_1, e_0) \cdot \mathrm{Res}_t(\tilde{f}_1, \tilde{f}_2).
\end{aligned}$$

Hence, we have $\check{G}_0 = \mathrm{Res}_t(\tilde{f}_1, e_0) \cdot G_0$, so there are even more extraneous factors than before due to the roots of $e_0$.

**Linearizing the problem.** The main idea to understand and eliminate the extraneous components that appeared in the example is to linearize the equations $g_1$ and $g_2$ by replacing the quadratic term $\langle y, y \rangle$ by a new variable $u$ (or more precisely $uy_0$ to keep the equations

homogeneous). This will make the results developed in Section 2 applicable. Geometrically, this means that we will pull back the spine curve to $\mathcal{Q}$ via the correspondence $\Phi$.

For a spine curve $\mathcal{E} \in \mathbb{R}^4_1$ we define a *proper* pre-image $\hat{\mathcal{E}}$ in the Lie quadric $\mathcal{Q}$ as the closure of the set $\hat{\mathcal{E}} = \Phi^{-1}(\mathcal{E})$ in $\mathcal{Q}$. It is immediate by (13) that the parametrization of $\hat{\mathcal{E}}$ is

$$\begin{array}{ccc} \mathbb{P}^1 & \dashrightarrow & \mathcal{Q} \subset \mathbb{P}^5 \\ t & \mapsto & (\langle e, e\rangle : e_0^2 : e_0e_1 : e_0e_2 : e_0e_3 : e_0e_4) \end{array} \tag{17}$$

We can now define the envelopes associated with this new spine curve as follows.

Definition 2.17. The variety $\mathcal{H}(\hat{\mathcal{E}}) \subset \mathbb{P}^5$ associated with $\hat{\mathcal{E}}$ is the hypersurface in $\mathbb{P}^5$ defined by the implicit equation $H(\hat{y}) = \mathrm{Res}_t(h_1, h_2)$ where $\hat{y} = (u : y_0 : y_1 : y_2 : y_3 : y_4)$ and

$$\begin{aligned} h_1(\hat{y}, t) &= -2[\hat{y}, \hat{\mathcal{E}}(t)] = ue_0^2 + y_0\langle e, e\rangle - 2\langle e_0e, y\rangle, \\ h_2(\hat{y}, t) &= \frac{\partial h_1(\hat{y}, t)}{\partial t} = -2[\hat{y}, \hat{\mathcal{E}}'(t)] \\ &= 2(ue_0e_0' + y_0\langle e', e\rangle - \langle (e_0e)', y\rangle). \end{aligned}$$

Similarly, the variety $\mathcal{H}_d(\hat{\mathcal{E}}) \subset \mathbb{P}^4$ is defined by the implicit equation

$$\begin{aligned} H_d(u, y_0, y_1, y_2, y_3) &= \mathrm{Res}_t(h_1|_{y_4=-dy_0}, h_2|_{y_4=-dy_0}) \\ &= \mathrm{Res}_t(h_1, h_2)|_{y_4=-dy_0}, \end{aligned}$$

i.e. the equation obtained by replacing $y_4$ in $H(\overline{y})$ by $-dy_0$, where $d \in \mathbb{R}$.

Of course this is nothing else than substituting $\langle y, y\rangle$ in $g_1$ and $g_2$ by $uy_0$ and dividing by $y_0$, so $g_i(\overline{y}) = h_i(\langle y, y\rangle, y_0^2, y_0y), i = 1, 2$, i.e. $g_i = h_i \circ \Phi^{-1}, i = 1, 2$. Now as an immediate corollary we obtain

Proposition 2.18. *With the notations as above we have*

$$G(\overline{y}) = H(\langle y, y\rangle, y_0^2, y_0y), \text{ i.e. } G = H \circ \Phi^{-1}, \text{ and} \tag{18}$$

$$G_d(y_0, y_1, y_2, y_3) = H_d(y_1^2 + y_2^2 + y_3^2 - d^2y_0^2, y_0^2, y_0y_1, y_0y_2, y_0y_3). \tag{19}$$

To sum up, we have defined two hypersurfaces as resultants of two quadratic forms: $\mathrm{Env}_d(\overline{\mathcal{E}}) \subset \mathbb{P}^3$, which are the offsets to the spine curve $\overline{\mathcal{E}}$, and $\mathcal{G}(\overline{\mathcal{E}}) \subset \mathbb{P}^4$, which can be interpreted as a parametrization of those offsets. As seen in an example, these definitions can lead to additional components which are against the geometric intuition, so it is desirable to give another definition which avoids those extra factors. To this end, we have linearized the problem by replacing the quadratic polynomials $g_1$ and $g_2$ by linear forms $h_1$ and $h_2$ by substituting the quadratic term by a new variable and have seen how to reverse this substitution. Geometrically, this means that we replace the hypersurfaces $\mathrm{Env}_d(\overline{\mathcal{E}})$ and $\mathcal{G}(\overline{\mathcal{E}})$ by hypersurfaces $\mathcal{H}_d(\hat{\mathcal{E}})$ and $\mathcal{H}(\hat{\mathcal{E}})$ in one dimension higher.

This has the advantage that we can now apply the technique of $\mu$-bases developed earlier to understand and eliminate the extraneous factors of $\mathcal{H}_d(\hat{\mathcal{E}})$ and $\mathcal{H}(\hat{\mathcal{E}})$ and then come back to $\mathbb{P}^3$ (resp. $\mathbb{P}^4$) with the substitution formulae of Proposition 2.18.

## 5. The dual variety, offsets, and the canal surface.

In this section, we will finally be able to define the canal surface $\mathcal{C}$ (and more general offsets to it) and the so-called dual variety $\Gamma(\overline{\mathcal{E}})$, which can be seen as a parametrization of the offsets to $\mathcal{C}$.

Up to the constant $-2$ the system $h_1 = h_2 = 0$ is equal to

$$\begin{cases} \left[\hat{y}, \hat{\mathcal{E}}(t)\right] = \hat{\mathcal{E}}(t)C\hat{y}^T = 0, \\ \left[\hat{y}, \hat{\mathcal{E}}'(t)\right] = \hat{\mathcal{E}}'(t)C\hat{y}^T = 0, \end{cases} \tag{20}$$

where the matrix $C$ is defined by the formula (11).

We can interpret the variety $\mathcal{H}(\hat{\mathcal{E}})$ defined by (20) as a dual variety to the curve $\hat{\mathcal{E}}$ with respect to the Lie quadric $\mathcal{Q}$, i.e. the dual variety to the curve $\hat{\mathcal{E}}(t)C$. Indeed, this dual variety consists of the hyperplanes which touch the curve $\hat{\mathcal{E}}(t)C$. The first equation in (20) means that the hyperplane contains the point $\hat{\mathcal{E}}(t)C$, the second equation means that the hyperplane contains the tangent vector $\hat{\mathcal{E}}'(t)C$ to the curve $\hat{\mathcal{E}}(t)C$.

In order to simplify notation we denote $E = \hat{\mathcal{E}}(t)C$ and $E' = \hat{\mathcal{E}}'(t)C$, or explicitly

$$\begin{aligned} E &= \left(-\frac{e_0^2}{2}, -\frac{\langle e, e\rangle}{2}, e_0e_1, e_0e_2, e_0e_3, -e_0e_4\right) \\ E' &= (-e_0e_0', -\langle e', e\rangle, e_0'e_1 + e_0e_1', e_0'e_2 + e_0e_2', \\ &\qquad e_0'e_3 + e_0e_3', -e_0'e_4 + e_0e_4') \end{aligned} \tag{21}$$

and we have that $\mathcal{H}(\hat{\mathcal{E}}) = \mathcal{S}_{E,E'}$ by (9). As we have seen in Section 2, this surface contains extraneous factors which correspond to the roots of the 2-minors of the matrix $W_{E,E'}$, but which can be eliminated by replacing $E, E'$ by a $\mu$-basis of the module $\langle E, E'\rangle$. It is thus natural to make the following definition.

Definition 2.19. We define the dual variety $\mathcal{V}(\hat{\mathcal{E}}) \subset \mathbb{P}^5$ to the curve $\hat{\mathcal{E}}$ as the hypersurface

$$\mathcal{V}(\hat{\mathcal{E}}) = \mathcal{S}_{\langle E,E'\rangle} \tag{22}$$

where $\langle E, E'\rangle$ is the module quasi-generated by $E$ and $E'$.

By the results of Section 2, it is immediate that $\mathcal{V}(\hat{\mathcal{E}}) \subset \mathcal{H}(\hat{\mathcal{E}})$ does not contain the components of $\mathcal{H}(\hat{\mathcal{E}})$ caused by parameters $t$ where $W_{E,E'}(t)$ is not of full rank or equivalently, where the intersection of

the hyperplanes defined by $h_1$ and $h_2$ is of codimension 1, i.e. the hyperplanes coincide. So we can deduce

PROPOSITION 2.20. *Let $E_1, E_2$ be a $\mu$-basis of the module quasi-generated by $E$ and $E'$ and let $k$ be the degree of the parametrization $E \wedge E'$ as in Section 2. Then*

$$k \cdot \deg\, \mathcal{V}(\hat{\mathcal{E}}) = \deg\, E_1 + \deg\, E_2 = \deg(E \wedge E') - \deg\, q_{E,E'},$$

*where $q_{E,E'} = \gcd(E \wedge E')$ and*

$$\operatorname{Res}_t(E_1 \cdot \hat{y}^T, E_2 \cdot \hat{y}^T) = F^k_{\mathcal{V}(\hat{\mathcal{E}})},$$

*where $F_{\mathcal{V}(\hat{\mathcal{E}})}$ is the implicit equation of $\mathcal{V}(\hat{\mathcal{E}})$. In particular, any matrix of the above resultant (e.g. Sylvester or Bézout) is a square representation matrix of $\mathcal{V}(\hat{\mathcal{E}})$.*

PROOF. It follows directly from Propositions 2.5 and 2.7. □

Of course, the same considerations can be applied to the hypersurfaces $\mathcal{H}_d(\hat{\mathcal{E}})$ and we make the analogous definitions. Substituting $y_4 = -dy_0$ in $h_1$ and $h_2$ corresponds to replacing $E$ and $E'$ by two linear forms

$$\begin{aligned} D &= \left(-\frac{e_0^2}{2}, -\frac{\langle e, e\rangle}{2} + de_0e_4, e_0e_1, e_0e_2, e_0e_3\right) \\ D' &= (-e_0e_0', -\langle e', e\rangle + d(e_0'e_4 - e_0e_4'), e_0'e_1 + e_0e_1', \\ &\qquad e_0'e_2 + e_0e_2', e_0'e_3 + e_0e_3') \end{aligned} \tag{23}$$

with $D, D' \in \mathbb{R}^5$. Now $\mathcal{H}_d(\hat{\mathcal{E}}) = \mathcal{S}_{D,D'}$ and one makes an analogous definition:

DEFINITION 2.21. We define the hypersurface $\mathcal{V}_d(\hat{\mathcal{E}})$ as

$$\mathcal{V}_d(\hat{\mathcal{E}}) = \mathcal{S}_{\langle D,D'\rangle} \subset \mathbb{P}^4 \tag{24}$$

where $\langle D, D'\rangle$ is the module quasi-generated by $D$ and $D'$.

In this case also, $\mathcal{V}_d(\hat{\mathcal{E}}) \subset \mathcal{H}_d(\hat{\mathcal{E}})$ does not contain extraneous factors due to the parameters $t$ where the rank of $W_{D,D'}(t)$ drops. At this point, it should be remarked that while we clearly always have

$$\mathcal{V}_d(\hat{\mathcal{E}}) \subset \mathcal{V}(\hat{\mathcal{E}}) \cap \{y_4 = -dy_0\}$$

this inclusion is not necessarily an equality (note that we had $\operatorname{Env}_d(\overline{\mathcal{E}}) = \mathcal{G}(\overline{\mathcal{E}}) \cap \{y_4 = -dy_0\}$ for the corresponding varieties). Analogously to Proposition 2.20 the following holds.

PROPOSITION 2.22. *Let $D_1, D_2$ be a $\mu$-basis of the module quasi-generated by $D$ and $D'$ and let $k$ be the degree of the parametrization $D \wedge D'$ as in Section 2. Then*

$$\deg\, \mathcal{V}_d(\hat{\mathcal{E}}) = \deg\, D_1 + \deg\, D_2 = \deg(D \wedge D') - \deg\, q_{D,D'},$$

*where* $q_{D,D'} = \gcd(D \wedge D')$ *and*

$$\operatorname{Res}_t(D_1 \cdot (u, y_0, y_1, y_2, y_3)^T, D_2 \cdot (u, y_0, y_1, y_2, y_3)^T) = F^k_{\mathcal{V}_d(\hat{\mathcal{E}})}$$

*where* $F_{\mathcal{V}_d(\hat{\mathcal{E}})}$ *is the implicit equation of* $\mathcal{V}_d(\hat{\mathcal{E}})$*. In particular, any matrix of the above resultant (e.g. Sylvester or Bézout) is a square representation matrix of* $\mathcal{V}_d(\hat{\mathcal{E}})$*.*

PROOF. It follows directly from Propositions 2.5 and 2.7. □

Finally, we can use the correspondance of Proposition 2.18 to define the canal surface.

DEFINITION 2.23. The Γ-hypersurface is defined as

$$\Gamma(\overline{\mathcal{E}}) = \Phi(\mathcal{V}(\hat{\mathcal{E}}) \cap \mathcal{Q}),$$

and the offset $\operatorname{Off}_d(\overline{\mathcal{E}})$ at distance d to the canal surface $\mathcal{C}$ is

$$\operatorname{Off}_d(\overline{\mathcal{E}}) = \Phi_0(\mathcal{V}_d(\hat{\mathcal{E}}) \cap \mathcal{Q}_d),$$

where $\mathcal{Q}_d = \{(u : y_0 : y_1 : y_2 : y_3) \in \mathbb{P}^4 \mid -uy_0 + y_1^2 + y_2^2 + y_3^2 - d^2 y_0^2 = 0\}$ and $\Phi_0(u, y_0, y_1, y_2, y_3) = (y_0, y_1, y_2, y_3)$. The canal surface itself is the special case $d = 0$ or in other words $\mathcal{C} = \operatorname{Off}_0(\overline{\mathcal{E}})$.

Note that the extraneous factors of $\mathcal{H}_d(\hat{\mathcal{E}})$ and $\mathcal{H}(\hat{\mathcal{E}})$ are in one-to-one correspondence with the extraneous factors of the corresponding hypersurfaces $\operatorname{Env}_d(\overline{\mathcal{E}})$ and $\mathcal{G}(\overline{\mathcal{E}})$ since they are caused by parameter values where the intersection of $h_1$ and $h_2$ (resp. $g_1$ and $g_2$) is of codimension one. So $\Gamma(\overline{\mathcal{E}})$ and $\mathcal{C}_d(\overline{\mathcal{E}})$ contain no such factors.

In this section and the previous one, many different geometric objects have been defined. We illustrate in the following diagram how they are related in order to make the situation clearer.

$$\begin{array}{ccccccc}
\mathbb{P}^4 & & \mathbb{P}^5 & & \mathbb{P}^5 & & \mathbb{P}^4 \\
\cup & & \cup & & \cup & & \cup \\
\mathcal{G}(\overline{\mathcal{E}}) & \xleftarrow{\Phi} & \mathcal{H}(\hat{\mathcal{E}}) \cap \mathcal{Q} & \supseteq & \mathcal{V}(\hat{\mathcal{E}}) \cap \mathcal{Q} & \xrightarrow{\Phi} & \Gamma(\overline{\mathcal{E}}) \\
\cup & & \cup & & \cup & & \cup \\
\operatorname{Env}_d(\overline{\mathcal{E}}) & \xleftarrow{\Phi_d} & \mathcal{H}_d(\hat{\mathcal{E}}) \cap \mathcal{Q}_d & \supseteq & \mathcal{V}_d(\hat{\mathcal{E}}) \cap \mathcal{Q}_d & \xrightarrow{\Phi_d} & \operatorname{Off}_d(\overline{\mathcal{E}}) \\
\cap & & \cap & & \cap & & \cap \\
\mathbb{P}^3 & & \mathbb{P}^4 & & \mathbb{P}^4 & & \mathbb{P}^3
\end{array} \tag{25}$$

Note that the hypersurfaces in the third row are included in the corresponding hypersurfaces in the second row. The first column is the naive definition of the objects to be studied: $\operatorname{Env}_d(\overline{\mathcal{E}})$ is more or less a $d$-offset to the canal offsets and $\mathcal{G}(\overline{\mathcal{E}})$ a hypersurface in one dimension higher containing all those offsets. However, they contain extraneous factors. So by passing to the second column, we linearize the hypersurfaces (i.e. we express them as resultants of linear forms) and can apply $\mu$-bases

to eliminate the extraneous factor, which gives the third column and finally go back down in dimension (by intersecting with $\mathcal{Q}$ and applying $\Phi$ to obtain the objects we are interested in: the offsets $\mathrm{Off}_d(\overline{\mathcal{E}})$ (in particular the canal surface $\mathcal{C} = \mathrm{Off}_0(\overline{\mathcal{E}})$) and the $\Gamma$-hypersurface.

**5.1. The implicit equation.** We can now describe how to compute powers of the implicit equations of the dual varieties $\mathcal{V}(\hat{\mathcal{E}})$ and $\mathcal{V}_d(\hat{\mathcal{E}})$, the hypersurface $\Gamma(\overline{\mathcal{E}})$ and the offsets surface $\mathcal{C}_d(\overline{\mathcal{E}})$. We should remark that these powers (which are the degrees of the parametrizations of the corresponding Plücker curves) are in a way inherent to the geometry of the problem, as we shall illustrate in Example 2.24. They can be interpreted as the number of times the surface is traced by the spine curve. Note also that this not necessarily due to the non-properness of the spine curve: Even for a proper spine curve it can happen that the canal surface (or its offsets) is multiply traced, as in Example 2.24.

ALGORITHM (implicit equations)

INPUT: a rational vector $e(t) \in \mathbb{R}(t)^4$ as in formula (4).

(1) Define $E, E' \in \mathbb{R}[t]^6$ as in formula (21) and $D, D' \in \mathbb{R}[t]^5$ as in formula (23).

(2) Compute a $\mu$-basis $E_1, E_2$ of the module $\langle E, E' \rangle$ and a $\mu$-basis $D_1, D_2$ of the module $\langle D, D' \rangle$ using the algorithm in Section 2.

(3) Set $F_{\mathcal{V}(\hat{\mathcal{E}})} = \mathrm{Res}_t(E_1 \cdot \hat{y}^T, E_2 \cdot \hat{y}^T)$ and $F_{\mathcal{V}_d(\hat{\mathcal{E}})} = \mathrm{Res}_t(D_1 \cdot (u, y_0, y_1, y_2, y_3)^T, D_2 \cdot (u, y_0, y_1, y_2, y_3)^T) = 0$.

(4) Let $F_{\Gamma(\overline{\mathcal{E}})}(y_0, y_1, y_2, y_3, y_4) = y_0^k F_{\mathcal{V}(\hat{\mathcal{E}})}((y_1^2 + y_2^2 + y_3^2 - y_4^2)/y_0, y_0, y_1, y_2, y_3, y_4)$, where $k$ is a minimal integer such that $F_{\Gamma(\overline{\mathcal{E}})}$ is a polynomial.
Similarly, set $F_{\mathcal{C}_d(\overline{\mathcal{E}})}(y_0, y_1, y_2, y_3) = y_0^k F_{\mathcal{V}_d(\hat{\mathcal{E}})}((y_1^2 + y_2^2 + y_3^2 - d^2 y_0^2)/y_0, y_0, y_1, y_2, y_3)$.

OUTPUT: $F_{\mathcal{V}(\hat{\mathcal{E}})}$, $F_{\mathcal{V}_d(\hat{\mathcal{E}})}$, $F_{\Gamma(\overline{\mathcal{E}})}$, and $F_{\mathcal{C}_d(\overline{\mathcal{E}})}$, which are powers of the implicit equation of the varieties $\mathcal{V}(\hat{\mathcal{E}})$, $\mathcal{V}_d(\hat{\mathcal{E}})$, $\Gamma(\overline{\mathcal{E}})$ and $\mathcal{C}_d(\overline{\mathcal{E}})$

Note that the affine parts of these equations can be obtained by replacing $y_0 = 1$ before the resultant computation.

**5.2. The parametrization of the dual variety.** We can describe the parametrization of $\mathcal{V}(\hat{\mathcal{E}})$. The hyperplane defined by the equation

$$\det(\hat{y}, E, E', a_1, a_2, a_3) = A_1u + A_2y_0 + \ldots + A_6y_4 = 0 \tag{26}$$

is tangent to the curve $E$ , $a_i \in \mathbb{R}^6, i = 1, 2, 3$ are three arbitrary points. By the definition a point on the dual variety $\mathcal{V}(\hat{\mathcal{E}})$ is $(A_1, ..., A_6)$. Define $D = (E, E', a_1, a_2, a_3)$ to be the $5 \times 6$ matrix with five rows $E, E', a_1, a_2, a_3$. Let $D_i, i = 1, ..., 6$ be $5 \times 5$ matrices obtained from $D$ by removing the i-th column, and let $\Delta_i = \det D_i$. Then using the Laplacian expansion by minors for the first row of the determinant (26) we obtain the parametrization of $\mathcal{V}(\hat{\mathcal{E}})$ as follows:

$$c(D) = (\Delta_1, -\Delta_2, \Delta_3, -\Delta_4, \Delta_5, -\Delta_6)/m \subset \mathcal{V}(\hat{\mathcal{E}}), \tag{27}$$

where $m = \gcd(\Delta_1, \ldots, \Delta_6)$. Here $t, a_1, a_2, a_3$ are arbitrary parameters.

## 6. Examples and special cases.

Example 2.24. Let us consider the following spine curve:

$$e(t) = \left(0, 0, \frac{8t}{1+t^2}, \frac{3-3t^2}{1+t^2}\right).$$

This is a proper parametrization of an ellipse in $\mathbb{R}^4$. For the Plücker vector $E \wedge E'$ we have $q_{E,E'} = 1$. If we run the $\mu$-basis algorithm with two input vectors $E, E'$ we get the output two vectors $E_1$ and $E_2$:

$$\begin{aligned} E_1 \cdot \hat{y}^T &= 4\,t^3y_3 + (-u - 41\,y_0)\,t^2 + 12\,ty_3 + 9\,y_0 - u - 6\,y_4, \\ E_2 \cdot \hat{y}^T &= (u - 9\,y_0 - 6\,y_4)\,t^3 - 12\,t^2y_3 + (41\,y_0 + u)\,t - 4\,y_3. \end{aligned}$$

Now we can find the implicit equation $G = \mathrm{Res}(E_1 \cdot \hat{y}^T, E_2 \cdot \hat{y}^T, t)$ of the dual variety $\mathcal{V}(\hat{\mathcal{E}})$. The polynomial $G$ contains 26 monomials and has degree 6. The equation of the hypersurface $\Gamma(\overline{\mathcal{E}})$ is the polynomial $F(y_0, ..., y_4) = y_0^2 G(\langle y, y\rangle/y_0, y_0, y_1, y_2, y_3, y_4)$ of degree 8. Since,

$$\begin{aligned} F(1, y_1, y_2, y_3, 0) &= (y_1{}^2 + 16 + y_2{}^2 + 8\,y_3 + y_3{}^2)(y_1{}^2 + y_2{}^2 + 16 \\ &\quad -8\,y_3 + y_3{}^2)(-225 + 25\,y_1{}^2 + 25\,y_2{}^2 + 9\,y_3{}^2)^2, \end{aligned}$$

the 0-envelope of the canal surface $\mathrm{Env}_0(\mathcal{E}) = \Gamma(\overline{\mathcal{E}}) \cap \{y_4 = 0\}$ is reducible. The canal surface $\mathcal{C}$ is the double ellipsoid of revolution $(-225 + 25\,y_1{}^2 + 25\,y_2{}^2 + 9\,y_3{}^2)^2$. Indeed, for the computation of $\mathcal{C}$ we should assume that the variable $y_4 = 0$ and to repeat the same steps as above. We should consider only the first 5 coordinates of the vectors $E, E'$, i.e. $D, D'$. But this time we see that the Plücker vector $D \wedge D'$ has a non-trivial common divisor $q_{D,D'} = t^2 - 1$. So, using the $\mu$-basis algorithm we find the $\mu$-basis $D_1, D_2$ for the input $D, D'$. In this case we see that $\deg D_1 = \deg D_2 = 2$. Now we find the resultant $\check{G} = \mathrm{Res}_t(D_1 \cdot \check{y}^T, D_2 \cdot \check{y}^T) = (16\,y_3{}^2 + 225\,y_0{}^2 - 25\,y_0u)^2$, where $\check{y} = (u, y_0, y_1, y_2, y_3)$. After the substitution $u = (y_1^2 + y_2^2 + y_3^2)/y_0$

we obtain the implicit equation of the canal surface the double ellipsoid $(-225+25\,{y_1}^2+25\,{y_2}^2+9\,{y_3}^2)^2$. We can see this geometrically, too. The point $e(t) \in \mathbb{R}^4$ corresponds to the sphere $S(e(t)) \in \mathbb{R}^3$ with a center on the $y_3$-axis. If $t \in [-1/2, 1/2]$ then the sphere $S(e(t))$ is tangent to the ellipsoid $EL = (-225+25\,{y_1}^2+25\,{y_2}^2+9\,{y_3}^2)$, and inside this ellipsoid. Moreover, the real envelope of the family $S(e(t)), t \in [-1/2, 1/2]$ is the ellipsoid $EL$. Note that the sphere $S(e(1/t))$ has the same center but the opposite radius to the sphere $S(e(t))$, i.e. it has the opposite orientation. Therefore, the real envelope of the family $S(e(t)), t \in (-\infty, -2] \cap [2, \infty)$ is the same ellipsoid $EL$. Hence, from the point of Laguerre geometry the envelope of the whole family $S(e(t))$ is the double ellipsoid $EL^2$. Note, that the d-offset to the canal surface, in this case is the d-offset to ellipsoid $EL$ and it has degree 8. For a detailed study and other examples of canal surfaces with a quadratic spine curve we recommend to look at the paper [**KZ07**].

Example 2.25. Consider the following spine curve in homogeneous form:

$$e(t, s) = \left(\frac{t+3\,s}{t}, \frac{t^3+4\,s^3}{ts^2}, 0, \frac{t^3+5\,s^3}{ts^2}\right)$$

Again we find that for the Plücker coordinate vector $E, E'$ we have $q_{E,E'} = 1$. If we run the $\mu$-basis algorithm we get the output of two vectors

$$\begin{aligned} E_1 &= (18\,s^3 - 2\,t^2 s + 2\,ts^2, 2\,ts^2, 9\,s^3 + 2\,ts^2, 12\,s^3, 0, 15\,s^3), \\ E_2 &= (-s\,(-s+4\,t)\,, s^2, s^2, 3\,t^2, 0, 3\,t^2), \end{aligned}$$

both of degree 2 and find the implicit equation $G$ of the dual variety $\mathcal{V}(\hat{\mathcal{E}})$ (it contains 51 monomials, so we do not present an explicit formula). For this example, we have $\deg \mathcal{C} = \deg \Gamma(\overline{\mathcal{E}}) = 7$, i.e. the implicit degree of the canal surface is 7.

Example 2.26. In the next example we take the following spine curve:

$$e(t) = \left(\frac{(1-t^2)^2}{(1+t^2)^2}, 2\,\frac{t\,(1-t^2)}{(1+t^2)^2}, 2\,\frac{t}{1+t^2}, 1\right)$$

The first three coordinates define the Viviani curve, i.e. it is intersection curve of the sphere and the tangent cylinder. In this case $\deg \mathcal{V}(\hat{\mathcal{E}}) = 6$. If we run the $\mu$-basis algorithm with two input vectors $E, E'$ we get output of two vectors

$$\begin{aligned} E_1 &= \left(0, 4+4\,t^2, 4-4\,t^2, 6\,t-2\,t^3, 6\,t+2\,t^3, 4+4\,t^2\right), \\ E_2 &= \left(0, 4\,t+4\,t^3, 4\,t\left(-1+t^2\right), 2-6\,t^2, 2+6\,t^2, 4\,t+4\,t^3\right), \end{aligned}$$

both of degree 3 and find the implicit equation $G$ of the dual variety $\mathcal{V}(\hat{\mathcal{E}})$ (it contains 58 monomials). For this example, we have $\deg \mathcal{C} = \deg \Gamma(\overline{\mathcal{E}}) = 10$, i.e. the implicit degree of the canal surface is 10.

CHAPTER 3

# Approximation complexes in the bihomogeneous case

Abstract. We show that the implicit equation of a surface in 3-dimensional projective space parametrized by bihomogeneous polynomials of bidegree $(d, d)$, for a given integer $d \geq 1$, can be represented and computed from the linear syzygies of its parametrization if the base points are isolated and form locally a complete intersection. The results in this chapter are joint work with Laurent Busé and have been published in [**BD07**].

## 1. Introduction

In [**BJ03**] and [**BC05**] it has been shown that the theory of approximation complexes can be used to represent rational surfaces defined by homogeneous parametrizations as non-square matrices built from linear syzygies. In this chapter our main objective is to develop this method for surfaces given by bihomogeneous parametrizations, which are of interest for a number of applications in geometric modelling and computer-aided design. We will show that also in this case the surface can be represented by a non-square matrix constructed by only using linear syzygies and we will explain how to efficiently compute this matrix with standard computer algebra systems.

This chapter can be seen as a prelude to the last one, in which we will generalize the method to a larger class of parametrizations (i.e. parametrizations over toric varieties), of which the parametrizations considered here are a special case. We have decided to treat them separately as a preparation for the general case, since this allows us to introduce the main concepts and ideas in a more accessible context and shows the historical development of our work. Moreover, some of the results obtained in this chapter are stronger than their counterparts for toric parametrizations. We will see that this is because in the bihomogeneous case the rings that are considered have some additional nice properties that make life easier than in the toric case.

Let us state precisely the problem we would like to solve. Let $\mathbb{K}$ be any field (all the varieties we will consider hereafter are understood to be taken over $\mathbb{K}$). We suppose given a rational map

$$\begin{array}{ccc} \mathbb{P}^1 \times \mathbb{P}^1 & \overset{\phi}{\dashrightarrow} & \mathbb{P}^3 \\ (s:u) \times (t:v) & \mapsto & (f_1 : f_2 : f_3 : f_4)(s,u,t,v) \end{array}$$

where the polynomials $f_1, \ldots, f_4$ are bihomogeneous of bidegree $(d, d)$, $d$ being a given positive integer, with respect to the homogeneous variables $(s : u)$ and $(t : v)$. We assume that

- $\phi$ parametrizes a surface $\mathscr{S}$ (which is equivalent to require that $\phi$ is a generically finite map onto its image) which is hence irreducible
- the greatest common divisor of $f_1, f_2, f_3, f_4$ is a non-zero constant which essentially requires the number of base points of $\phi$ to be finite (possibly zero).

We aim to find a representation of $\mathscr{S}$ in terms of linear syzygies of $f_1, f_2, f_3$ and $f_4$ similar to the known ones for plane curves and for space surfaces parametrized by the projective plane.

The chapter is organized as follows. In Section 2 we give an equivalent formulation of our problem which replaces the given $\mathbb{N} \times \mathbb{N}$-graduation by a single $\mathbb{N}$-graduation. In Section 3 we will introduce an associated approximation complex that will be used in Section 3.3 to prove our main result. Then an algorithmic version is detailed in Section 4, as well as an illustrative example.

## 2. The Segre embedding

It is well-known that $\mathbb{P}^1 \times \mathbb{P}^1$ can be embedded in $\mathbb{P}^3$ through the so-called *Segre embedding*

$$\begin{array}{ccc} \mathbb{P}^1 \times \mathbb{P}^1 & \overset{\rho}{\dashrightarrow} & \mathbb{P}^3 \\ (s : u) \times (t : v) & \mapsto & (st : sv : ut : uv). \end{array}$$

We denote by $\mathscr{H}$ its image, which is an irreducible surface of degree 2 in $\mathbb{P}^3$, whose equation in the coordinates $X_1, X_2, X_3, X_4$ of $\mathbb{P}^3$ is known to be $X_1X_4 - X_2X_3$. Our strategy to solve our implicitization problem is to reparametrize the surface $\mathscr{S}$ by $\mathscr{H} \subset \mathbb{P}^3$, that is to say to consider $\mathscr{S}$ as the closed image of the map $\psi$ from $\mathscr{H}$ to $\mathbb{P}^3$ fitting in the commutative diagram

(28)
$$\begin{array}{ccc} \mathbb{P}^1 \times \mathbb{P}^1 & \overset{\phi}{\dashrightarrow} & \mathbb{P}^3 \\ \downarrow \rho & \nearrow_{\psi} & \\ \mathscr{H} & & \end{array}$$

In the rest of this chapter we will use the map $\psi = \phi \circ \rho^{-1}$ to implicitize $\mathscr{S}$, which has the advantage of replacing the $\mathbb{N} \times \mathbb{N}$-graduation of $\mathbb{P}^1 \times \mathbb{P}^1$ by a single $\mathbb{N}$-graduation. In order to justify this approach we need to describe explicitly the algebraic counterparts of the maps in the above diagram.

We begin with the map $\phi$. The polynomial ring $\mathbb{K}[s,u]$ is canonically $\mathbb{N}$-graded,

$$\mathbb{K}[s,u] = \bigoplus_{n\in\mathbb{N}} \mathbb{K}[s,u]_n = \mathbb{K}[s,u]_0 \oplus \mathbb{K}[s,u]_1 \oplus \mathbb{K}[s,u]_2 \oplus \dots$$

where $\mathbb{K}[s,u]_i$ denotes the degree $i$ homogeneous component of $\mathbb{K}[s,u]$, and its homogeneous spectrum is the projective line, i.e. $\mathrm{Proj}(\mathbb{K}[s,u]) = \mathbb{P}^1_{\mathbb{K}}$. Of course, the same is true for the polynomial ring $\mathbb{K}[t,v]$. Now, consider the $\mathbb{N}$-graded $\mathbb{K}$-algebra

$$S := \bigoplus_{n\in\mathbb{N}} (\mathbb{K}[s,u]_n \otimes_{\mathbb{K}} \mathbb{K}[t,v]_n) \subset \mathbb{K}[s,u] \otimes_{\mathbb{K}} \mathbb{K}[t,v]$$

which is finitely generated by $S_1$ as an $S_0$-algebra. Then $\mathbb{P}^1 \times \mathbb{P}^1$ is the homogeneous spectrum $\mathrm{Proj}(S)$ of $S$. Introducing new indeterminates $T_1, T_2, T_3, T_4$, the map $\phi$ is hence induced by the graded $k$-algebra morphism

$$\begin{array}{rcl} \mathbb{K}[T_1,T_2,T_3,T_4] & \xrightarrow{p} & S \\ T_i & \mapsto & f_i(s,u,t,v) \quad i = 1,\dots,4. \end{array}$$

By [**BJ03**, Theorem 2.1], $\ker(p) \subset \mathbb{K}[T_1,T_2,T_3,T_4]$ is the defining ideal of the closed image of $\phi$ in $\mathbb{P}^3 = \mathrm{Proj}(\mathbb{K}[T_1,\dots,T_4])$; it is prime (since $S$ is a domain) and principal (since it is of codimension one by hypothesis and $\mathbb{K}[T_1,T_2,T_3,T_4]$ is factorial), i.e. any generator of $\ker(p)$ gives an equation of $\mathscr{S}$.

We now turn to the Segre embedding $\rho$. As we did for the map $\phi$ (note that the Segre embedding is itself a parametrization of a surface in projective space) the map $\rho$ is induced by the graded $k$-algebra morphism

$$\begin{array}{rcl} \mathbb{K}[X_1,X_2,X_3,X_4] & \xrightarrow{\theta} & S \\ X_1 & \mapsto & st \\ X_2 & \mapsto & sv \\ X_3 & \mapsto & ut \\ X_4 & \mapsto & uv. \end{array}$$

However, in this case $\theta$ is surjective and graded (it preserves the degree). Moreover, it is easy to see[1] that its kernel is the principal ideal $(X_1X_4 - X_2X_3) \subset \mathbb{K}[X_1,X_2,X_3,X_4]$. Therefore, $\theta$ induces a graded isomorphism of $\mathbb{N}$-graded $\mathbb{K}$-algebras

$$\bar{\theta} : A := \mathbb{K}[X_1,X_2,X_3,X_4]/(X_1X_4 - X_2X_3) \xrightarrow{\sim} S$$

[1]We clearly have $(X_1X_4 - X_2X_3) \subset \ker(\theta)$. Now, if $P \in \ker(\theta)$ we deduce by a pseudo-euclidean division that there exists $N \in \mathbb{N}^\star$ such that

$$X_4^N P = Q(X_1,\dots,X_4)(X_1X_4 - X_2X_3) + R(X_2,X_3,X_4).$$

But then $R \in \ker(\theta)$ and it is obvious that we have $\mathbb{K}[X_2,X_3,X_4] \cap \ker(\theta) = 0$.

which identifies $\mathbb{P}^1\times\mathbb{P}^1 = \mathrm{Proj}(S)$ with the Segre variety $\mathscr{H} = \mathrm{Proj}(A) \subset \mathbb{P}^3 = \mathrm{Proj}(\mathbb{K}[X_1, X_2, X_3, X_4])$.

We are now ready to describe $\psi$. This map is of the form

$$\begin{array}{rcl} \mathscr{H} \subset \mathbb{P}^3 & \xrightarrow{\psi} & \mathbb{P}^3 \\ (X_1 : X_2 : X_3 : X_4) & \mapsto & (g_1 : g_2 : g_3 : g_4)(X_1, X_2, X_3, X_4) \end{array} \tag{29}$$

where $g_1, g_2, g_3, g_4$ are homogeneous polynomials of the same degree in $\mathbb{K}[X_1, X_2, X_3, X_4]$. By the graded isomorphism $\bar{\theta}$, it follows $\deg(\phi) = \deg(\psi)$ (we understand co-restriction to $\mathscr{S}$) and also that the $g_i$'s must have degree $d$. To give an algorithmic construction we just have to determine the inverse map of $\bar{\theta}$. To do this, for all $n \in \mathbb{N}$ define the integer $k_{i,j}^{(n)} := \max(0, n-i-j)$ and consider the map

$$\begin{array}{rcl} S_n & \xrightarrow{\omega_n} & \mathbb{K}[X_1, X_2, X_3, X_4]_n \\ s^i u^{n-i} t^j v^{n-j} & \mapsto & X_1^{i+j-n+k_{i,j}^{(n)}} X_2^{n-j-k_{i,j}^{(n)}} X_3^{n-i-k_{i,j}^{(n)}} X_4^{k_{i,j}^{(n)}} \end{array}$$

(for all couples $(i,j) \in \{0,\dots,n\}^2$). Then, we define the map

$$\omega := \bigoplus_{n\in\mathbb{N}} \omega_n : S \to \mathbb{K}[X_1, X_2, X_3, X_4]$$

which induces the inverse of $\bar{\theta}$ by passing to the quotient ring $A = \mathbb{K}[X_1, X_2, X_3, X_4]/(X_1X_4 - X_2X_3)$ (this is easy to check). Observe also that no monomial in the image of $\omega$ is divisible by $X_1X_4$, so our representation of the inverse of $\bar{\theta}$ can be thought of as already reduced. Moreover, the coefficients of the $f_i$'s and the $g_i$'s are in correspondence: only the monomials are changed by $\omega$.

Therefore, we proved

PROPOSITION 3.1. *Defining for all $i = 1, 2, 3, 4$ the homogeneous polynomial*

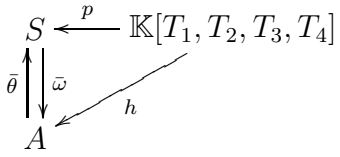
$$g_i(X_1, X_2, X_3, X_4) := \omega(f_i(s, u, t, v)) \in \mathbb{K}[X_1, X_2, X_3, X_4]_d,$$

*the map* (29) *is a parametrization of the surface $\mathscr{S} \subset \mathbb{P}^3$ with the property that* $\deg(\psi) = \deg(\phi)$.

Furthermore, we actually proved that our initial problem, namely the implicitization of $\phi$ in terms of syzygies, is equivalent to the same problem with the parametrization $\psi$ which is induced by the map

$$\begin{array}{rcl} \mathbb{K}[T_1, T_2, T_3, T_4] & \xrightarrow{h} & A \\ T_i & \mapsto & g_i(X_1, X_2, X_3, X_4). \end{array}$$

This can be summarized by the following commutative diagram, which is the algebraic translation of the diagram (28).




This shows that the syzygies of the $f_i$'s over $S$ are in correspondence with the syzygies of the $g_i$'s over $A$, in particular $\ker(h) = \ker(p)$. Moreover, it also shows that the base points of the parametrization $\phi$ are in one-to-one correspondence with the base points of the parametrization $\psi$ and that their local structure (complete intersection, multiplicity, etc.) is preserved by this correspondence.

Another interesting remark is the following: By [**BJ03**, Theorem 2.5], we deduce that we have the equality

$$\deg(\psi)\deg(\mathscr{S}) = \deg(\mathscr{H})d^2 - \sum_{\mathfrak{p}\in V(g_1,\dots,g_4)\cap\mathscr{H}\subset\mathbb{P}^3} e_{\mathfrak{p}}$$

where $e_{\mathfrak{p}}$ denotes the algebraic multiplicity (in the sense of Hilbert-Samuel). Since it is immediate to check that $\deg(\mathscr{H}) = 2$ we recover the well-known formula of intersection theory (see [**Fu84**, Prop. 4.4] or [**Co01**, Appendix]):

$$\deg(\phi)\deg(\mathscr{S}) = 2d^2 - \sum_{\mathfrak{p}\in V(f_1,\dots,f_4)\subset\mathbb{P}^1\times\mathbb{P}^1} e_{\mathfrak{p}}. \tag{30}$$

Therefore, *in the rest of this chapter we will focus on the implicitization of $\psi$ by means of linear syzygies*, which is a completely equivalent problem to our initial one.

## 3. The approximation complex

For simplicity, we will denote by $X_i$ the classes of the variables in the quotient ring $A = \mathbb{K}[\underline{X}]/(X_1X_4 - X_2X_3)$, where $\underline{X}$ stands for the sequence $X_1, X_2, X_3, X_4$. Recall that $A$ is canonically graded, each variable having weight 1. Let $I = (g_1, g_2, g_3, g_4) \subset A$ be the ideal generated by the $g_i$'s. We give a brief definition of the approximation complex of cycles associated to the sequence $g_1, g_2, g_3, g_4$ over $A$. This has been studied in depth in [**HSV83**], see also [**Va94**]. Under the right conditions, this complex yields free resolutions of certain graded parts of the symmetric algebra $\mathrm{Sym}_A(I)$, which is one of the main motivations for its study. Another essential feature of this complex is that - unlike the Koszul complex - its homology depends only on the ideal $(g_1, \dots, g_4)$, not on the generators $g_i$. Here is the construction:

We consider the Koszul complex $(K_\bullet(\underline{g}, A), d_\bullet)$ associated to $g_1, \ldots, g_4$ over $A$ and denote $Z_i = \ker(d_i)$ and $B_i = \mathrm{im}(d_{i+1})$. It is of the form

$$A(-4d) \xrightarrow{d_4} A(-3d)^4 \xrightarrow{d_3} A(-2d)^6 \xrightarrow{d_2} A(-d)^4 \xrightarrow{d_1} A$$

where the differentials are matrices with $\pm g_1, \ldots, \pm g_4$ as non-zero entries. We introduce new variables $T_1, \ldots, T_4$ and set $\mathcal{Z}_i = Z_i(i \cdot d) \otimes_A A[\underline{T}]$, which we will consider as bigraded $A[\underline{T}]$-modules (one grading is induced by the grading of $A$, the other one comes from setting $\deg(T_i) = 1$ for all $i$). Now the approximation complex of cycles $(\mathcal{Z}_\bullet(\underline{g}, A), e_\bullet)$, or simply $\mathcal{Z}_\bullet$, is the complex

$$0 \to \mathcal{Z}_3(-3) \xrightarrow{e_3} \mathcal{Z}_2(-2) \xrightarrow{e_2} \mathcal{Z}_1(-1) \xrightarrow{e_1} \mathcal{Z}_0$$

where the differentials $e_\bullet$ are obtained by replacing $g_i$ by $T_i$ for all $i$ in the matrices of $d_\bullet$ (note that $\mathcal{Z}_4 = 0$, since $d_4$ is injective). It is an important remark that

$$\begin{aligned} \mathrm{im}(e_1) &= \left\{ \sum_{i=1}^4 p_i T_i \mid p_i \in A[\underline{T}], \sum_{i=1}^4 p_i g_i = 0 \right\} \\ &= \left( \sum_{i=1}^4 p_i T_i \mid p_i \in A, \sum_{i=1}^4 p_i g_i = 0 \right) \subset A[\underline{T}] \end{aligned} \tag{31}$$

and therefore $H_0(\mathcal{Z}_\bullet) = A[\underline{T}]/\mathrm{im}(e_1) \simeq \mathrm{Sym}_A(I)$. Note that the degree shifts indicated in the complex above are with respect to the grading given by the $T_i$'s, while the degree shifts with respect to the grading of $A$ are already contained in our definition of the $\mathcal{Z}_i$'s. From now on, when we take the degree $\nu$ part of the approximation complex, denoted $(\mathcal{Z}_\bullet)_\nu$, it should always be understood to be taken with respect to the grading induced by $A$. Hereafter we denote by $\mathfrak{m}$ the ideal $(X_1, X_2, X_3, X_4) \subset A$.

**3.1. Acyclicity criterion.** Let us first define the canonical module, a notion we will use in this section.

DEFINITION 3.2. Let $R = \mathbb{K}[X_1, \ldots, X_n]$, $I$ an ideal of $R$ and suppose that $M = R/I$ is of dimension $d$. Then the canonical module of $R$ is defined as $\omega_R = R[-n]$ and

$$\omega_M = \mathrm{Ext}_R^{n-d}(M, R[-n])$$

is the canonical module $\omega_M$ of $M$.

This is the same definition as in [**Ch00**] and will be sufficient in our context. See [**BH93**] or [**Ei95**] for detailed treatments of canonical modules and a more general definition. Our first concern is to show that the approximation complex of cycles $\mathcal{Z}_\bullet(g_1, \ldots, g_4; A)$ is acyclic under suitable assumptions. We have, similarly to [**BC05**, Lemma 2], the following

LEMMA 3.3. *Suppose that $I = (g_1, g_2, g_3, g_4) \subset A$ is of codimension at least 2, and let $\mathscr{P} := \mathrm{Proj}(A/I) \subset \mathscr{H}$. Then the following are equivalent:*

*(i) $\mathcal{Z}_\bullet$ is acyclic,*
*(ii) $\mathcal{Z}_\bullet$ is acyclic outside $V(\mathfrak{m})$,*
*(iii) $\mathscr{P}$ is locally defined by 3 equations (i.e. locally an almost complete intersection).*

PROOF. The proof is very similar to [**BC05**, Lemma 2]; the only difference is that $A$ is not a polynomial ring here, but it is still a Gorenstein ring which is the main required property for $A$. Observe that the lemma is unaffected by an extension of the base field, so one may assume that $\mathbb{K}$ is infinite.

By [**HSV83**, Theorem 12.9], we know that $\mathcal{Z}_\bullet$ is acyclic (resp. acyclic outside $V(\mathfrak{m})$) if and only if $I$ is generated by a proper sequence (resp. $\mathscr{P}$ is locally defined by a proper sequence). Recall that a sequence $a_1, \ldots, a_n$ of elements in a commutative ring $B$ is a *proper sequence* if

$$a_{i+1} H_j(a_1, \ldots, a_i; B) = 0 \quad \text{for } i = 0, \ldots, n-1 \text{ and } j > 0,$$

where the $H_j$'s denote the homology groups of the corresponding Koszul complex.

It is clear that (i) implies (ii). Assuming (ii), we will now deduce that $\mathscr{P}$ is locally defined by a proper sequence. As explained in [**BC05**, Lemma 2], one can choose $h_1, h_2, h_3, h_4$ to be sufficiently generic linear combinations of the $g_i$'s such that

- $(h_1, \ldots, h_4) = (g_1, \ldots, g_4) \subset A$,
- $h_1, h_2$ is an $A$-regular sequence, which implies that $h_1$, $h_2$, $h_3$ is a proper sequence in $A$,
- $h_1, \ldots, h_4$ form a proper sequence outside $V(\mathfrak{m})$.

By [**BH93**, Theorem 1.6.16], we have

$$H_1(h_1, h_2, h_3; A) \simeq \mathrm{Ext}^2_A(A/(h_1, h_2, h_3), A)$$

and since $A$ is Gorenstein (for it is a complete intersection), i.e. isomorphic to its canonical module [**BH93**, Theorem 3.3.7], then

$$H_1(h_1, h_2, h_3; A) \simeq \mathrm{Ext}^2_A(A/J, A) \simeq \omega_{A/J} \tag{32}$$

outside $V(\mathfrak{m})$, where $\omega_-$ stands for the canonical module and $J := (h_1, h_2, h_3) \subset A$. Since the annihilator of $\omega_{A/J}$ over $A$ is $(J : \mathfrak{m}^\infty) \subset A$ (observe that $A/J$ defines isolated points and use for instance [**Ei95**, Corollary 21.3]), we deduce that $h_4 \in (J : \mathfrak{m}^\infty)$, that is to say that $\mathscr{P}$ is locally defined by 3 equations.

Now, assume (iii). Similarly to what we did above, one can find $h_1, \ldots, h_4$ sufficiently generic linear combinations of the $g_i$'s so that $h_1, h_2$ is an $A$-regular sequence and $h_1, h_2, h_3$ define $\mathscr{P}$. It follows that $h_4 \in (J : \mathfrak{m}^\infty) \subset A$, where $J := (h_1, h_2, h_3) \subset A$, and hence (32)

implies that $h_4$ annihilates $H_1(h_1, h_2, h_3; A)$; it follows that $h_1, \ldots, h_4$ form a proper sequence in $A$, so $\mathcal{Z}_\bullet$ is acyclic. □

As soon as the base points (if there are any) of the parametrization $\psi$ (or equivalently $\phi$) are isolated and locally defined by 3 equations, then its associated approximation complex of cycles is acyclic. Therefore, it can be used to compute and represent the codimension one part of the annihilator of the $A[T_1, \ldots, T_4]$-module $H^0(\mathcal{Z}_\bullet)$ which is nothing but the symmetric algebra $\mathrm{Sym}_A(I)$. In the following, we will use the local cohomology $H^i_{\mathfrak{m}}(M)$ of an $A$-module $M$. A detailed exposition of this concept is beyond the scope of this work, see [**BS98**] for a comprehensive introduction to the subject. Let us just state that it can be obtained as the homology of the so-called Čech-complex $\mathcal{C}^\bullet_{\mathfrak{m}}(M)$, whose terms are direct sums of localizations of $M$, or more precisely $\mathcal{C}^0_{\mathfrak{m}}(M) = M$ and for all $p = 1, \ldots, 4$ one has

$$\mathcal{C}^p_{\mathfrak{m}}(M) = \bigoplus_{1 \leq j_1 < \ldots < j_p \leq 4} M_{X_{j_1} X_{j_2} \cdots X_{j_p}}.$$

See [**BS98**] for more details and an explicit construction of the differentials of this complex.

Lemma 3.4. *Suppose that $\mathscr{P} := \mathrm{Proj}(A/I)$ has dimension $\leq 0$ and is locally defined by 3 equations. If $\eta$ is an integer such that*

$$H^0_{\mathfrak{m}}(\mathrm{Sym}_A(I))_\nu = 0 \quad \textit{for all } \nu \geq \eta,$$

*then, for all $\nu \geq \eta$ we have*

$$\mathrm{ann}_{\mathbb{K}[\underline{T}]}(\mathrm{Sym}_A(I)_\nu) = \mathrm{ann}_{\mathbb{K}[\underline{T}]}(\mathrm{Sym}_A(I)_\eta) \subseteq \ker(h).$$

*Moreover, the above inclusion is an equality if $\mathscr{P}$ is locally defined by 2 equations.*

Proof. For all $\nu \geq \eta$, the equality

$$\mathrm{ann}_{\mathbb{K}[\underline{T}]}(\mathrm{Sym}_A(I)_\nu) = \mathrm{ann}_{\mathbb{K}[\underline{T}]}(\mathrm{Sym}_A(I)_\eta)$$

is proven in [**BJ03**, Proposition 5.1] for $A = \mathbb{K}[\underline{X}]$. However, the same proof can be applied without modifications to our setting: The key property used in the proof is the fact that the canonical map $A_1 \otimes A_n \to A_{n+1}$ is surjective and this is also valid for $A = \mathbb{K}[\underline{X}]/(X_1X_4 - X_2X_3)$. Moreover, by (31) we have that $\mathrm{ann}_{\mathbb{K}[\underline{T}]}(\mathrm{Sym}_A(I)_\nu) \neq 0$ for $\nu \gg 0$ if and only if $\mathscr{P}$ is locally generated by at most 3 equations, and in this case it is clear that it is contained in $\ker(h)$. Finally, if $\mathscr{P}$ is locally defined by at most 2 equations, meaning that $\mathscr{P}$ is locally a complete intersection, then $I$ is of linear type outside $V(\mathfrak{m})$ (use for instance [**BJ03**, Propositions 4.1 and 4.5]) which shows the last claimed equality as proven in [**BJ03**, Proposition 5.1]. □

In other words, if the base points of the parametrization are isolated and locally complete intersections then certain graded parts of the approximation complex $\mathcal{Z}_\bullet$ yield a way to compute an implicit equation of $\mathscr{S}$. Our next task is to explicitly describe the saturation index of the symmetric algebra, i.e. the integer $\eta$ appearing in LEMMA 3.4. This will provide us with the key tool for developing the algorithm presented in Section 4.

**3.2. The saturation index.** For any ideal $J$ of $A$ we denote by $J^{\text{sat}}$ the saturation of $J$ with respect to the ideal $\mathfrak{m}$, i.e. $J^{\text{sat}} := (J :_A \mathfrak{m}^\infty) \subset A$. Also, we recall that if $M$ is a $\mathbb{N}$-graded $B$-module, where $B$ is a $\mathbb{N}$-graded ring, its initial degree is defined as

$$\text{indeg}(M) := \min\{\nu \in \mathbb{N} : M_\nu \neq 0\} \geq 0.$$

With these notations, we have

THEOREM 3.5. *If $\mathscr{P} := \text{Proj}(A/I)$ is a zero-dimensional scheme (i.e. supported on a finite number of points, possibly zero) then*

$$H^0_{\mathfrak{m}}(\text{Sym}_A(I))_\nu = 0 \qquad \forall \nu \geq 2d - 1 - \text{indeg}(I^{\text{sat}}).$$

The proof of this theorem is actually similar to the proof of [**BC05**, Theorem 4]. The difference is that in our case the ring $A$ is not a polynomial ring but a quotient ring. So to validate the proof of [**BC05**, Theorem 4] we have to make explicit the local cohomology and the dualizing module of $A$ which is, as a complete intersection, a Gorenstein ring (the key property for what follows). We state these results in a little more general case for the sake of clarity, our case being the special case $n = 4$, $k = \mathbb{K}$, and $f = X_1X_4 - X_2X_3$:

PROPOSITION 3.6. *Let $k$ be a commutative Noetherian ring and $C := k[X_1, \ldots, X_n]$, with $n \geq 1$, which is canonically graded by $\deg(X_i) = 1$ for all $i = 1, \ldots, n$. Suppose given a homogeneous polynomial $f$ of degree $r \geq 1$ and consider the graded quotient ring $B := C/(f)$. The following properties hold:*

- *$\omega_B \simeq B(-n + r)$, a graded isomorphism where $\omega_B$ stands for the canonical module of $B$,*
- *$H^i_{\mathfrak{m}}(B) = 0$ if $i \neq n - 1$ and for all $\nu \in \mathbb{Z}$*

$$H^{n-1}_{\mathfrak{m}}(B)_\nu \simeq B(-n + r)_{-\nu},$$

- *if $K_\bullet$ denotes the Koszul complex associated to a given sequence $(a_1, \ldots, a_s)$ of homogeneous elements in $B$ of degree $d_1, \ldots, d_s$ respectively, then we have the isomorphisms*

$$H^{n-1}_{\mathfrak{m}}(K_\bullet)_\nu \simeq \text{Hom}_{B/\mathfrak{m}}(K_{s-\bullet}(\sum_{i=1}^{s} d_i - n + r)_{-\nu}, B/\mathfrak{m}).$$

PROOF. To prove the first claim, we first recall that we have $\omega_C \simeq C(-n)$. Then, [**BH93**, Corollary 3.6.14] shows that

$$\omega_B \simeq (\omega_C / f.\omega_C)(r) \simeq B(-n+r).$$

For the second claim, we recall that the local cohomology of $C$ is well-known: $H^i_{\mathfrak{m}}(C) = 0$ for all $i \neq n$ and

$$H^n_{\mathfrak{m}}(C)_\nu \simeq C_{-n-\nu} \tag{33}$$

for all $\nu \in \mathbb{Z}$. Now, the exact sequence

$$0 \to C(-r) \xrightarrow{\times f} C \to B \to 0$$

whose long exact cohomology sequence contains the segments

$$H^j_{\mathfrak{m}}(C) \to H^j_{\mathfrak{m}}(B) \to H^{j+1}_{\mathfrak{m}}(C(-r))$$

implies that $H^j_{\mathfrak{m}}(B) = 0$ for all $j < n-1$ as for $j+1 < n$ both the left and the right hand side vanish. Furthermore, the segment

$$0 \to H^{n-1}_{\mathfrak{m}}(B) \to H^n_{\mathfrak{m}}(C(-r)) \to H^n_{\mathfrak{m}}(C)$$

taken in degree $\nu$ shows

$$H^{n-1}_{\mathfrak{m}}(B)_\nu = \ker\left(H^n_{\mathfrak{m}}(C(-r))_\nu \to H^n_{\mathfrak{m}}(C)_\nu\right).$$

By the self-duality of the Koszul complex and (33) this later equals exactly $B_{-\nu-n+r}$. Finally, since $\dim(C) = n$ we have $\dim(B) = n-1$ which implies that $H^j_{\mathfrak{m}}(B) = 0$ for $j > n-1$ by [**BH93**, Theorem 3.5.7].

The third claim is a direct generalization of the classical property

$$H^n_{\mathfrak{m}}(K_\bullet)_\nu \simeq \mathrm{Hom}_{C/\mathfrak{m}}(K_{s-\bullet}(\sum_{i=1}^{s} d_i - n)_{-\nu}, C/\mathfrak{m}).$$

The only thing which changes is the shift by $r$ in the canonical module of $B$ and the dimension of $B$ which is $n-1$ whereas $\dim(C) = n$. □

PROOF OF THEOREM 3.5. We consider the two spectral sequences associated to the double complex $H^\bullet_{\mathfrak{m}}(\mathcal{Z}_\bullet)$:

$$\begin{array}{ccccccccc}
0 & \to & \mathcal{C}^0_{\mathfrak{m}}(\mathcal{Z}_3) & \to & \mathcal{C}^0_{\mathfrak{m}}(\mathcal{Z}_2) & \to & \mathcal{C}^0_{\mathfrak{m}}(\mathcal{Z}_1) & \to & \mathcal{C}^0_{\mathfrak{m}}(\mathcal{Z}_0) \to 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
0 & \to & \mathcal{C}^1_{\mathfrak{m}}(\mathcal{Z}_3) & \to & \mathcal{C}^1_{\mathfrak{m}}(\mathcal{Z}_2) & \to & \mathcal{C}^1_{\mathfrak{m}}(\mathcal{Z}_1) & \to & \mathcal{C}^1_{\mathfrak{m}}(\mathcal{Z}_0) \to 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
 & & \vdots & & \vdots & & \vdots & & \vdots \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
0 & \to & \mathcal{C}^4_{\mathfrak{m}}(\mathcal{Z}_3) & \to & \mathcal{C}^4_{\mathfrak{m}}(\mathcal{Z}_2) & \to & \mathcal{C}^4_{\mathfrak{m}}(\mathcal{Z}_1) & \to & \mathcal{C}^4_{\mathfrak{m}}(\mathcal{Z}_0) \to 0
\end{array}$$

They both converge to the hypercohomology of $\mathcal{Z}_\bullet$. One of them stabilizes at level two with:

$$ {}_2{}'E_q^p = {}_\infty{}'E_q^p = \begin{cases} H^p_{\mathfrak{m}}(H_q(\mathcal{Z}_\bullet)) & \text{for } p = 0, 1 \text{ and } q > 0 \\ H^p_{\mathfrak{m}}(\mathrm{Sym}_A(I)) & \text{for } q = 0 \\ 0 & \text{else.} \end{cases} $$

and the other one gives at level one:

$$ {}_1{}''E_q^p = H^p_{\mathfrak{m}}(Z_q)[qd] \otimes_A A[\underline{T}](-q). $$

As explained in [**BC05**, Theorem 4], the comparison of these two spectral sequences and [**BC05**, Lemma 1] show[2] that $H^0_{\mathfrak{m}}(\mathrm{Sym}_A(I))_\nu$ is the zero module as soon as $({}_1{}''E_p^p)_\nu$ vanishes for $p = 2, 3$. Moreover, setting $—^\star := \mathrm{Homgr}_A(—, A/\mathfrak{m})$, we have the graded isomorphisms

$$ {}_1{}''E_3^3 \simeq (A/I)^\star[2-d] \otimes_A A[\underline{T}](-3) $$

and

$$ {}_1{}''E_2^2 \simeq (I^{\mathrm{sat}}/I)^\star[2-2d] \otimes A[\underline{T}](-2). $$

It follows that $({}_1{}''E_2^2)_\nu$ and $({}_1{}''E_3^3)_\nu$ vanish simultaneously if

$$ \nu > \min(d-2, 2d-2-\mathrm{indeg}(I^{\mathrm{sat}}/I)). $$

This is true whenever $\nu \geq \nu_0 := 2d-1-\mathrm{indeg}(I^{\mathrm{sat}})$, since the identity $\min(d, \mathrm{indeg}(I^{\mathrm{sat}}/I)) = \mathrm{indeg}(I^{\mathrm{sat}})$ holds. □

REMARK 3.7. Since $I$ is generated in degree $d$ and $I \subset I^{\mathrm{sat}}$ we have the inequality $0 \leq \mathrm{indeg}(I^{\mathrm{sat}}) \leq d$. It follows that

$$ d-1 \leq 2d-1-\mathrm{indeg}(I^{\mathrm{sat}}) \leq 2d-1. $$

The lower bound is reached whenever the ideal $I$ is saturated (meaning $I = I^{\mathrm{sat}}$) and the higher bound corresponds to the absence of base points of the parametrization.

**3.3. The main result.** We now have all the tools necessary at our disposal and can proceed to the main result of this chapter. But before, recall that there are two distinct notions of multiplicity for a base point $\mathfrak{p} \in V(I) \cap \mathscr{H} \subset \mathbb{P}^3$: the algebraic multiplicity denoted $e_{\mathfrak{p}}$ and the geometric multiplicity denoted $d_{\mathfrak{p}}$ (see for instance [**BJ03**, §2.2] for more details).

THEOREM 3.8. *Assume that* $\dim \mathscr{P} := \mathrm{Proj}(A/I) \leq 0$ *and that* $\mathscr{P}$ *is locally an almost complete intersection (i.e. locally defined by 3 equations). Then, for every integer*

$$ \nu \geq \nu_0 := 2d-1-\mathrm{indeg}(I^{\mathrm{sat}}) $$

[2]Note that [**BC05**, Lemma 1] can be applied verbatim in our case (modulo some little change on the degree shifts that we will describe below) because of PROPOSITION 3.6.

*the determinant $D$ of the complex $(\mathcal{Z}_\bullet)_\nu$ of $\mathbb{K}[\underline{T}]$-modules (which is unique up to multiplication by a non-zero constant in $\mathbb{K}$) is a non-zero homogeneous element in $\mathbb{K}[\underline{T}]$, independent of $\nu \geq \nu_0$ and of degree*

$$2d^2 - \sum_{\mathfrak{p}\in V(I)\cap\mathscr{H}\subset\mathbb{P}^3} d_{\mathfrak{p}}$$

*such that $D = F^{\deg(\psi)}G$ where $F$ is the implicit equation of $\mathscr{S}$, $G$ is coprime with $F$ and $\deg(G) = \sum_{\mathfrak{p}\in V(I)\cap\mathscr{H}}(e_{\mathfrak{p}} - d_{\mathfrak{p}})$.*

*Moreover, $G \in \mathbb{K}\setminus\{0\}$ if and only if $\mathscr{P}$ is locally a complete intersection (i.e. locally defined by 2 equations).*

PROOF. First of all, observe that $D$ is independent of $\nu$ by THEOREM 3.5. It is an homogeneous element of $\mathbb{K}[\underline{T}]$ because $(\mathcal{Z}_\bullet)_\nu$ is a graded complex of $\mathbb{K}[\underline{T}]$-modules and it is non-zero because $\mathscr{P}$ is locally an almost complete intersection, a fact we already used in LEMMA 3.4.

The computation of $\deg(D)$ can be done as in [**BC05**, Theorem 4]: For $\nu \gg 0$ we have

$$\deg(D) = \dim(Z_1)_{\nu+d} - 2\dim(Z_2)_{\nu+2d} + 3\dim(Z_3)_{\nu+3d}.$$

In the case where all the $H_i$'s, with $i > 0$, vanish then $\deg(D) = 2d^2$. If $H_1$ and $H_2$ are non-zero, then they contribute to the above quantity for

$$\begin{aligned}(34)\quad &\dim(H_1)_{\nu+d} - \dim(H_2)_{\nu+d} - 2\dim(H_2)_{\nu+2d}\\ &\qquad = \dim(H_0)_{\nu+d} - 2\dim(H_2)_{\nu+2d} = -deg\mathscr{P}\end{aligned}$$

where we assume that $\nu \gg 0$, since $H_2 \simeq \omega_{A/I}$ (this can be proven as in [**Ch00**, Fact 1.13], because $A$ is Gorenstein). Therefore, we deduce that

$$(35)\qquad \deg(D) = 2d^2 - \deg\mathscr{P} = 2d^2 - \sum_{\mathfrak{p}\in V(I)\cap\mathscr{H}\subset\mathbb{P}^3} d_{\mathfrak{p}}.$$

Now, setting $\mathfrak{q} := \ker(h)$ and using standard properties of determinants of complexes we compute

$$\begin{aligned}[\det((\mathcal{Z}_\bullet)_\nu)] &= \operatorname{div}(H_0(\mathcal{Z}_\bullet))\\ &= \operatorname{div}(\operatorname{Sym}_A(I)_\nu)\\ &= \sum_{\mathfrak{p}\text{ prime, }\operatorname{codim}(\mathfrak{p})=1} \operatorname{length}((\operatorname{Sym}_A(I)_\nu)_{\mathfrak{p}})\cdot[\mathfrak{p}]\\ &= \operatorname{length}((\operatorname{Sym}_A(I)_\nu)_{\mathfrak{q}})\cdot[\mathfrak{q}] + \cdots.\end{aligned}$$

Since $\operatorname{length}((\operatorname{Sym}_A(I)_\nu)_{\mathfrak{q}}) = \deg(\psi)$ as proved in [**BJ03**, Theorem 5.2], we deduce that $D = F^{\deg(\psi)}G$ where $G$ does not divide $F$.

Finally, using equations (30) and (35) we deduce that

$$\deg(G) = \sum_{\mathfrak{p} \in V(I) \cap \mathscr{H}} (e_{\mathfrak{p}} - d_{\mathfrak{p}}),$$

and it is well-known that $e_{\mathfrak{p}} \geq d_{\mathfrak{p}}$ with equality if and only if the point $\mathfrak{p}$ is locally a complete intersection. □

Recall that the determinant of the complex $(\mathcal{Z}_\bullet)_\nu$ can either be obtained as an alternating product over some sub-determinants of the matrices appearing in the complex or as a gcd of maximal minors of the first map in the $(\mathcal{Z}_\bullet)_\nu$-complex (we refer to [**GKZ94**, Appendix A] for a thorough presentation of determinants of complexes, in which this is proven). So as an immediate corollary we have

COROLLARY 3.9. *Assume that $\mathscr{P}$ is a local complete intersection and let $M$ be the matrix of the first map $(\mathcal{Z}_1)_\nu \to (\mathcal{Z}_0)_\nu$ of the complex $\mathcal{Z}_\bullet$. Then $M$ is a representation matrix for the surface $\mathscr{S}$.*

We will explicitly construct this matrix $M$ in the next section. As we have already mentioned, the matrix $M$ can be used to decide if a given point $P$ lies on the surface. It suffices to evaluate $M$ in this point, as the rank of $M$ drops if and only if $P$ belongs to the surface. One can also see this in the following way: For a commutative ring $R$ and a morphism $\alpha : R^m \to R^n$ with $m \geq n$ we always have

$$\operatorname{ann}_R(\operatorname{coker}(\alpha))^n \subseteq I_n(\alpha) \subseteq \operatorname{ann}_R(\operatorname{coker}(\alpha))$$

where $I_n(\alpha)$ denotes the ideal generated by the maximal minors of the matrix of $\alpha$, i.e. the principal Fitting ideal of $\alpha$ (see for instance [**Ei95**, Proposition 20.7]). Ours is the special case $R = \mathbb{K}[\underline{T}]$ and $\alpha$ is the first map in $(\mathcal{Z}_\bullet)_\nu$, i.e. the one induced by $e_1$, and hence $\operatorname{coker}(\alpha) = \operatorname{Sym}_A(I)_\nu$. Geometrically, this means that the maximal minors of $M$ define the hypersurface $\mathscr{S}$ by LEMMA 3.4, and consequently, the points for which the rank of $M$ drops are exactly those belonging to $\mathscr{S}$.

## 4. Algorithm

In order to show explicitly how the theoretical results from the previous sections are used in practice, we formulate an algorithm for the actual computation of the matrix representing the implicit equation. It is efficient and easy to implement, as it consists basically of the resolution of a linear system. We give only the essential steps, see [**BC05**, Section 3] for a more detailed description of a very similar algorithm.

- Given four bihomogeneous polynomials $f_1, f_2, f_3, f_4$ of degree $d$, define the homogeneous polynomials $g_1, g_2, g_3, g_4 \in A = \mathbb{K}[\underline{X}]/(X_1X_4 - X_2X_3)$ of the same degree by setting $g_i = \omega(f_i)$, where $\omega$ is the isomorphism defined in Section 2.

- Find the solution space of the linear system (over $\mathbb{K}$) defined by

$$\sum_{i\in\{1,\dots,4\}} a_i g_i = 0$$

  where $(a_1, a_2, a_3, a_4) \in (A_{\nu_0})^4$ and $\nu_0 = 2d-1-\text{indeg}(I^{\text{sat}})$, i.e. one writes the equation with respect to a basis of $A_{\nu_0+d}$ and compares the coefficients. The solution space can be represented by a kernel matrix $N$ of size $l \times 4\dim_{\mathbb{K}}(A_{\nu_0})$-matrix $N$, where $l < \dim_{\mathbb{K}}(A_{\nu_0+d})$ and each row represents a basis vector of the solution space. The first $k := \dim_{\mathbb{K}}(A_{\nu_0})$ columns represent the coefficients of $a_1$, the next $k$ coefficients $a_2$, etc.
- For $i \in \{1, \dots, 4\}$, let $M_i$ be the $k \times k$-matrix $T_i \cdot \text{Id}_k$. Then the $k \times l$-matrix

$$M := \begin{pmatrix} M_1 & \cdots & M_4 \end{pmatrix} \cdot N^t$$

  is the matrix of the first map of the graded part $(\mathcal{Z}_\bullet)_{\nu_0}$ of the approximation complex.

As we proved, in the case where the base points of the parametrization $\phi$ are isolated and locally complete intersections, $M$ represents the surface $\mathscr{S}$. Also, the *gcd* of the maximal minors (of size $k$) of $M$ equals its implicit equation.

## 5. Comments and conclusion

We have presented a new approach to compute an implicit representation in terms of linear syzygies for a surface in $\mathbb{P}^3$ parametrized by bihomogeneous polynomials of bidegree $(d, d)$, $d \geq 1$, under the assumption that the base points are isolated and locally complete intersections. This result, along with the similar ones for parametrizations over the projective plane, shows that in many cases it is not necessary to use quadratic syzygies in order to represent the implicit equation of a surface. We should point out that this method has the advantages of being valid in a very general setting (we have neither assumed birationality nor made other additional assumptions on the parametrization) and of working well in the presence of base points. Furthermore, the matrix representing the surface can be computed in a very efficient way.

Of course, requiring the bidegree to be unmixed is rather restrictive. In the following chapter we will generalize the method not only for bihomogeneous parametrizations of bidegree $(d_1, d_2)$ with $d_1, d_2 \geq 1$, but also for parametrizations over toric varieties. At this point, let us discuss some ideas one might have to generalize to the mixed case:

- Putting weights on the variables in $S$ will not give us good properties for $S$, for instance $S$ will not be generated by $S_1$ as an $S_0$ algebra in general.
- Considering the bidegree $(\max(d_1,d_2),\max(d_1,d_2))$ is not possible because it introduces a base point locus of positive dimension and we will lose the acyclicity of the approximation complex.
- One way to come back to unmixed bidegree is to make the substitutions

  $$s \leftarrow s^{\mathrm{lcm}(d_1,d_2)/d_1} \text{ and } t \leftarrow t^{\mathrm{lcm}(d_1,d_2)/d_2}.$$

  Everything works fine in this case, but we are not representing $F^{\deg(\psi)}$, but $F^{\deg(\psi)\mathrm{lcm}(d_1,d_2)/\gcd(d_1,d_2)}$ which is not optimal, as it increases the size of the matrices involved. For instance, we could treat Example 10 from [**KD06**] in this way. It is a surface of bidegree (2,3) defined by

  $$\begin{aligned} f_1 &= (t+t^2)(s-1)^2+(1+st-s^2t)(t-1)^2 \\ f_2 &= (-t-t^2)(s-1)^2+(-1+st+s^2t)(t-1)^2 \\ f_3 &= (t-t^2)(s-1)^2+(-1-st+s^2t)(t-1)^2 \\ f_4 &= (t+t^2)(s-1)^2+(-1-st-s^2t)(t-1)^2 \end{aligned}$$

  By replacing $s$ by $s^3$ and $t$ by $t^2$, we obtain a parametrization of bidegree $(6,6)$ and $F^6$ can indeed be computed in degree $\nu \geq 2\cdot 6-1-6=5$ of the approximation complex as the *gcd* of the maximal minors of a $42\times 36$-matrix, whereas in the original paper it was computed as the determinant of a $5\times 5$-matrix.
- In [**AHW05**], the method of moving planes and quadrics (which yields a square representation matrix constructed with linear and quadratic syzygies) has been generalized to parametrizations over $\mathbb{P}^1\times\mathbb{P}^1$ by taking into account the bigraded structure of $S$. A similar approach might also work for the method of approximation complexes and would consist of generalizing the results in [**BJ03**] to a bigraded ring instead of a graded ring.

We have not pursued any of these ideas any further, but in the next chapter we will follow yet another approach, which is to use a more general Segre-Veronese map to embed $\mathbb{P}^1\times\mathbb{P}^1$ (or a toric variety) as a surface in some $\mathbb{P}^m$. In general, this will not be a hypersurface and the corresponding ring $A$ will be more complicated (for example, it is not necessarily Gorenstein). Nevertheless, we will see that the method is also valid in that context, but different tools (essentially from combinatorial commutative algebra) are needed to explain why.

CHAPTER 4

# Approximation complexes in the toric case

ABSTRACT. In this chapter we extend the methods introduced in the previous chapter to surfaces in $\mathbb{P}^3$ parametrized over a 2-dimensional toric variety $\mathscr{T}$, i.e. we show that such a surface can be represented and computed from the linear syzygies of its parametrization if the base points are finite in number and form locally a complete intersection. We treat the important example $\mathscr{T} = \mathbb{P}^1 \times \mathbb{P}^1$, a special case of which we have considered in the previous chapter, in detail and give numerous examples to show that this is a major improvement of the previous results. This chapter is joint work with Nicolás Botbol and Alicia Dickenstein.

## 1. Introduction

In practical applications in computer-aided design and geometric modeling, surfaces are rarely given by homogeneous maps. Most often, they are defined as rational maps in affine space of the form

$$\begin{array}{ccc} \mathbb{A}^2 & \overset{\phi}{\dashrightarrow} & \mathbb{A}^3 \\ (s,t) & \mapsto & \left(\dfrac{f_1}{f_4}, \dfrac{f_2}{f_4}, \dfrac{f_3}{f_4}\right) \end{array}$$

where $f_i \in \mathbb{K}[s,t]$ are polynomials such that $\gcd(f_1, \ldots, f_4) = 1$ and the field $\mathbb{K}$ is usually $\mathbb{R}$. In order to apply implicitization methods based on syzygies or resultants, one has to homogenize them and consider them as projective maps

$$\begin{array}{ccc} \mathscr{T} & \overset{\psi}{\dashrightarrow} & \mathbb{P}^3 \\ P & \mapsto & (g_1(P) : g_2(P) : g_3(P) : g_4(P)) \end{array}$$

where $\mathscr{T}$ is a 2-dimensional projective variety and the $g_i$ are homogenized versions of their affine counterparts $f_i$. In other words, $\mathscr{T}$ is a suitable compactification of the affine space $\mathbb{A}^2$. In previous publications, the method of approximation complexes has been developed for the case $\mathscr{T} = \mathbb{P}^2$, see for example [**BJ03**], [**BC05**], and [**Ch06**], and as we have seen in Chapter 3 for the case $\mathscr{T} = \mathbb{P}^1 \times \mathbb{P}^1$ if the parametrization is bihomogeneous of degree $(d,d)$. However, for a given parametrization $\phi$, these two varieties are not necessarily the best choice of a compactification of the affine plane, since they do not always reflect well the combinatorial structure of the polynomials $f_1, \ldots, f_4$. In this chapter we will extend the method to a much larger class of varieties

(toric varieties of dimension 2) and we will see that this generalization allows us to choose a "good" compactification of $\mathbb{A}^2$ depending on the polynomials $f_1, \ldots, f_4$, which makes the method applicable in cases where it failed over $\mathbb{P}^2$ or $\mathbb{P}^1 \times \mathbb{P}^1$ and that it is significantly more efficient and leads to much smaller matrix representations.

There are essentially two reasons why a certain compactification can be "bad": First, the homogenization with respect to a given variety can introduce base points which are not local complete intersections and in this case the method will fail, as seen in Chapter 3. Second, a given compactification might not be well adapted to the polynomials $f_1, \ldots, f_4$ and lead to an avoidable increase in computational complexity. In the example section at the end of the chapter, we will illustrate more precisely what this means.

Note that the idea of using toric varieties to improve implicitization methods has been used in [**KD06**] to modify the classical method of implicitization with resultants by using the toric resultant and in which they introduce a toric generalization of the method of moving planes and quadrics, which has been developed for instance in [**SC95**], [**BCD03**], and [**AHW05**]. Later, we shall compare this method in some examples with the method developed here.

The main idea of the approach is similar to the one in Section 3.2: We use a (general) toric embedding to consider our domain as a 2-dimensional toric variety contained in a higher-dimensional projective space. Contrary to the previous chapter, it will not be a hypersurface and its coordinate ring will usually not be Gorenstein, which means that we have to give new proofs for some of the results in which this property was used. We proceed to establish the necessary homological tools and in particular to derive bounds on local cohomology. After that, we will see that we can deduce the validity of the method from previous results and illustrate how it works in examples. An implementation of the method in Macaulay2 [**M2**] for the important special case $\mathscr{T} = \mathbb{P}^1 \times \mathbb{P}^1$ is included in the Appendix.

## 2. Toric embeddings

Let $\mathbb{K}$ be a field. All the varieties considered hereafter are understood to be taken over $\mathbb{K}$. We suppose given a rational map

$$\begin{array}{ccc} \mathbb{A}^2 & \overset{\phi}{\dashrightarrow} & \mathbb{P}^3 \\ (s,t) & \mapsto & (f_1 : f_2 : f_3 : f_4)(s,t) \end{array}$$

where $f_i \in \mathbb{K}[s,t]$ are polynomials. We assume that

- $\phi$ is a generically finite map onto its image and hence parametrizes an irreducible surface $\mathscr{S} \subset \mathbb{P}^3$

- $\gcd(f_1, \ldots, f_4) = 1$, which means that there are only finitely many base points.

We briefly introduce some basic notions from toric geometry. These constructions are investigated in more detail in [**KD06**, Sect. 2], [**Co03b**], and [**GKZ94**, Ch. 5 and 6].

DEFINITION 4.1. Let $p = \sum_{(\alpha,\beta)\in\mathbb{Z}^2} p_{\alpha,\beta} s^\alpha t^\beta \in \mathbb{K}[s,t]$. We define the support $\mathrm{Supp}(p)$ to be the set of all the exponents which appear in $p$, i.e.

$$\mathrm{Supp}(p) = \{(\alpha,\beta) \in \mathbb{Z}^2 \mid p_{\alpha,\beta} \neq 0\} \subset \mathbb{Z}^2$$

The Newton polytope $\mathrm{N}(f) \subset \mathbb{R}^2$, where $f = (f_1, f_2, f_3, f_4)$, is defined as the convex hull of the union $\bigcup_i \mathrm{Supp}(f_i)$ in $\mathbb{R}^2$ of the supports of the $f_i$. In other words, $\mathrm{N}(f)$ is the smallest convex polygon in $\mathbb{R}^2$ containing all the exponents appearing in one of the $f_i$.
Furthermore, let $d \in \mathbb{N}$ be the biggest integer such that $d \cdot \mathrm{N}'(f) = \mathrm{N}(f)$ and that the vertices of $\mathrm{N}'(f)$ are in $\mathbb{Z}^2$. In other words, $\mathrm{N}'(f)$ is the smallest possible homothety of $\mathrm{N}(f)$ with integer vertices.

Then $\mathrm{N}'(f)$ defines a two dimensional projective toric variety $\mathscr{T} \subseteq \mathbb{P}^m$, as explained in [**Co03b**], where $m+1$ is the cardinality of $\mathrm{N}'(f) \cap \mathbb{Z}^2$. It is defined as the closed image of the embedding

$$\begin{array}{rcl} \mathbb{A}^2 & \overset{\rho}{\dashrightarrow} & \mathbb{P}^m \\ (s,t) & \mapsto & (\ldots : s^i t^j : \ldots) \end{array}$$

where $(i,j) \in \mathrm{N}'(f) \cap \mathbb{Z}^2$ and the rational map $\phi$ factorizes through $\mathscr{T}$ in the following way

(36)
$$\begin{array}{ccc} \mathbb{A}^2 & \overset{\phi}{\dashrightarrow} & \mathbb{P}^3 \\ \downarrow \rho & \nearrow_{\psi} & \\ \mathscr{T} & & \end{array}$$

where $\psi$ is given by four polynomials $g_1, \ldots, g_4$ of degree $d$ in $m$ variables. Thus, we have extended the affine parametrization $\phi$ to a parametrization $\psi$ of $\mathscr{S}$ over the projective variety $\mathscr{T}$

$$\begin{array}{rcl} \mathscr{T} & \overset{\psi}{\dashrightarrow} & \mathbb{P}^3 \\ P & \mapsto & (g_1(P) : \ldots : g_4(P)) \end{array}$$

for which we will adapt the method of approximation complexes. This map induces an application between the homogeneous coordinate rings

$$\begin{array}{rcl} \mathbb{K}[T_1, T_2, T_3, T_4] & \overset{h}{\to} & A \\ T_i & \mapsto & g_i(X_0, \ldots, X_m) \end{array}$$

where $A = \mathbb{K}[X_0, \ldots, X_m]/I(\mathscr{T})$ is the homogeneous coordinate ring of $\mathscr{T}$. The ideal $I(\mathscr{T})$ is prime, so $A$ is a domain. Note that the

$X_k$ correspond to monomials $s^i t^j$ and the ideal $I(\mathscr{T})$ is the ideal of relations between these monomials. By the same arguments as in the previous chapter, $\ker(h)$ is by hypothesis a principal ideal generated by the implicit equation of $\mathscr{S}$. Later, we will need the following well-known degree formula.

PROPOSITION 4.2.

$$\deg(\psi)\deg(\mathscr{S}) = \mathrm{Area}(\mathrm{N}(f)) - \sum_{\mathfrak{p}\in V(g_1,\dots,g_4)\subset\mathscr{T}} e_{\mathfrak{p}}$$

*where* $\mathrm{Area}(\mathrm{N}(f))$ *is twice the Euclidean area of* $\mathrm{N}(f)$*, i.e. the normalized area of the polygon and* $e_{\mathfrak{p}}$ *is the multiplicity of the base point* $\mathfrak{p}$*.*

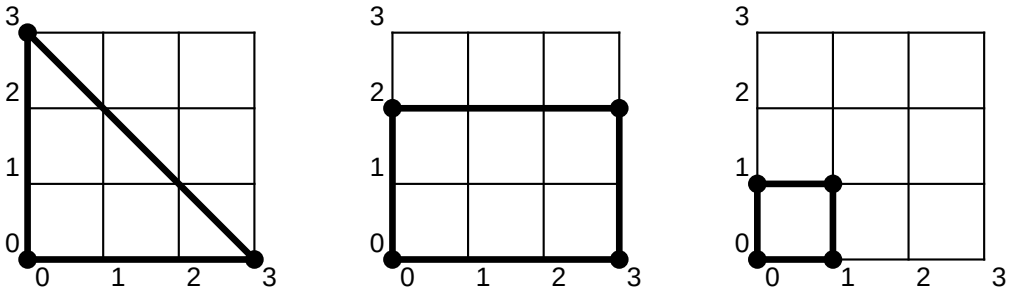
PROOF. This is the statement of [**KD06**, Prop. 1]. See also [**Co01**, Appendix]. □

The toric ideals $I(\mathscr{T})$ are very well understood and there exist highly efficient software systems to compute their Gröbner bases, for example [**4ti2**].

Instead of $\mathrm{N}'(f)$ we could actually have chosen any other homothety of $\mathrm{N}(f)$ and the method of approximation complexes will work in the same way. In particular, we could choose $\mathrm{N}(f)$ itself, in which case the $g_i$ will become linear forms, compare [**KD06**, Sect. 2]. We will see in Section 5 that $\mathrm{N}'(f)$ is always the better choice; for the moment let us just state that a smaller polygon leads to a less complicated coordinate ring but to a higher degree of the $g_i$ and that the advantages of the former outweigh the inconveniences of the latter.

Alternatively, one may choose any polygon $Q$ such that a multiple $d \cdot Q$, $d \in \mathbb{N}$, contains $\mathrm{N}(f)$. There is a priori no general rule for the choice for such a polygon $Q$, but we will see in the example section that in some cases there are better choices than $\mathrm{N}'(f)$, provided that this compactification does not lead to "bad" base points.

Intuitively, the surface $\mathscr{T}$ should be understood to be the smallest compactification of $\mathbb{A}^2$ through which the map $\phi$ factorizes, so in a way it respects the geometry of the map best and is a natural candidate. The cases $\mathscr{T} = \mathbb{P}^2$ and $\mathscr{T} = \mathbb{P}^1 \times \mathbb{P}^1$ correspond to the following Newton polytopes.

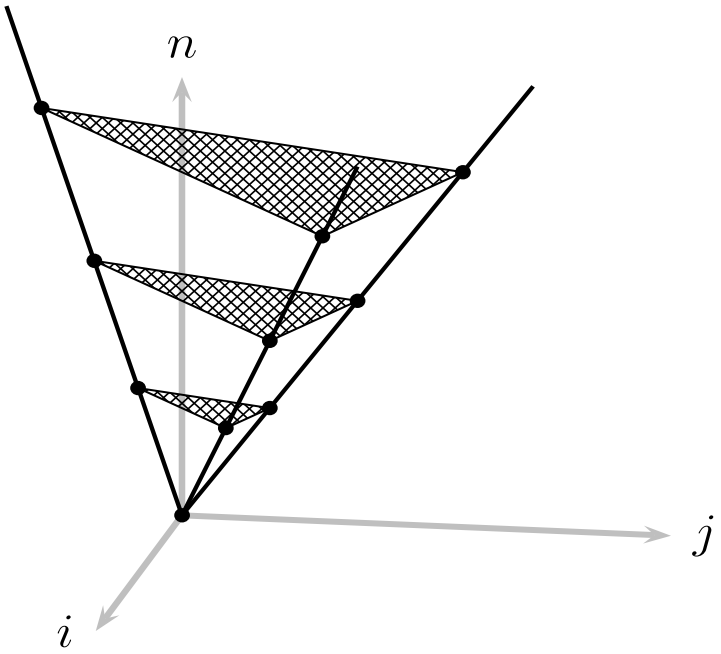


The first polytope is the Newton polytope of a dense homogeneous parametrization of degree 3, the second one corresponds to a bihomogeneous parametrization of bidegree $(3, 2)$ and the last one is exactly the case treated in the previous chapter, i.e. the smallest homothety of the Newton polytope of a bihomogeneous parametrization of bidegree $(d, d)$.

**2.1. The combinatorial structure of the ring $A$.** We can describe the ring $A$ in a more combinatorial way, which will enable us to study its properties in more detail. Let $C$ be the cone generated by the polytope $\mathrm{N}'(f)$ in $\mathbb{Z}^3$, i.e.

$$C = \{(i, j, n) \mid (i, j) \in n \cdot \mathrm{N}'(f) \cap \mathbb{Z}^2\} \subseteq \mathbb{Z}^3$$

which means that at each height $n$ we have a homothety of $\mathrm{N}'(f)$ by the factor $n$. As an illustration, consider the following picture of the cone $C$:




Note that only the integer points in the above triangles belong to $C$. Now we can associate an affine semigroup ring $\mathbb{K}[C]$ to this cone: one takes the $\mathbb{K}$-vector space freely generated by the elements of $C$ and equips it with a natural multiplication, which is induced by the addition of vectors in $\mathbb{Z}^3$, see [**BH93**, Ch. 6] for more details. It is actually

a graded $\mathbb{K}$-algebra, with the grading being induced by the height $n$, i.e. by the decomposition $C = \bigcup_n C_n$, where $C_n = \{(i, j, n) \mid (i, j) \in n \cdot \mathrm{N}'(f) \cap \mathbb{Z}^2\}$. Recall that the variable $X_k$ in $A$ stands for a monomial $s^i t^j$, which we can identify with a the point $(i, j, 1) \in C$, or in other words, we can identify $\mathrm{N}'(f) \cap \mathbb{Z}^2$ with $C_1$. The multiplication of two monomials in $A$ corresponds to the addition of two vectors in $C$. For instance, in the picture, $C_n$ is the triangle at height $n$, which represents the monomials in $A$ of degree $n$ and the multiplication of, say, a monomial of degree 1 with a monomial of degree 2 means adding a point of the lowest triangle with a point on the middle one, which gives a point in the triangle at the top, which represents a monomial of degree 3.

It is easy to verify that the above correspondence extends to a graded isomorphism of $\mathbb{K}$-algebras between $A$ and $\mathbb{K}[C]$ by observing that the relations of $I(\mathscr{T})$ correspond to different decompositions of an element of $C_n$ as the sum of elements of smaller degree, so we actually have

$$A \simeq \mathbb{K}[C]$$

We should note that these considerations are no longer true in higher dimension. This is because in dimension $\geq 3$ there exist non-normal lattice polytopes, see [**MS05**, Ex. 12.6]. Exploiting this combinatorial description of the ring $A$ we can deduce some algebraic properties.

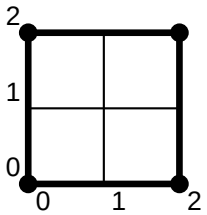
Lemma 4.3.

- *The homogeneous coordinate ring $A$ of the toric variety $\mathscr{T}$ is an affine normal semigroup ring.*
- *$A$ is Cohen-Macaulay.*
- *The canonical module $\omega_A$ of $A$ is the ideal generated by the monomials that correspond to points in the interior of $C$.*

Proof. The first bullet point is a direct consequence of [**BH93**, Prop. 6.1.2 and 6.1.4], since $C$ is a normal semigroup. The second and third bullet points are the statement of [**BH93**, Prop. 6.3.5]. □

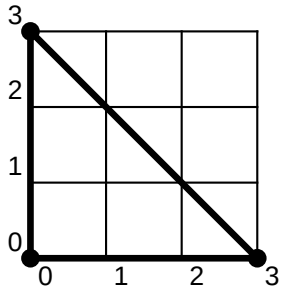
Recall that the canonical module was defined in Definition 3.2. The third bullet point in the lemma shows that $A$ is Gorenstein if and only if the first $C_i$ with non-empty interior (either $i = 1$, $i = 2$, or $i = 3$) contains exactly one point. In this case, it is actually easy to see the isomorphism between $\omega_A$ and $A$ geometrically: It is nothing else than the translation that moves the point in the interior of $C_i$ to the origin.

Remember that in the previous chapter, i.e. for bihomogeneous parametizations of bidegree $(d, d)$, the polygon $C_2$ was the following:



So in this case, $A$ was Gorenstein and we could use this property in the proofs. In the general case, we have to do without this property, so some of the proofs have to be modified.

Similarly, for $\mathbb{P}^2$ the polygons $C_1$ and $C_2$ have no interior points and $C_3$ contains one interior point:




This shows that in this case, which is the one treated in [**BJ03**] and [**BC05**], the ring $A$ is also Gorenstein.

## 3. Homological tools

**3.1. Overview of approximation complexes.** The construction of the approximation complex $\mathcal{Z}_\bullet$ is exactly the same as in Section 3.3, but we repeat it here for completeness' sake and to fix notation, compare also [**HSV83**], [**Va94**], and [**BJ03**].

We will denote by $X_i$ the class of the variable in the homogeneous coordinate ring $A = \mathbb{K}[\underline{X}]/J$ of $\mathscr{T}$, where $J = I(\mathscr{T})$ and $\underline{X}$ stands for the sequence $X_0, \ldots, X_m$. We consider $A$ as a graded ring, each variable having weight 1. Let $I = (g_1, g_2, g_3, g_4) \subset A$ be the ideal generated by the $g_i$, recall that $d = \deg(g_i)$.
We consider the Koszul complex $(K_\bullet(\underline{g}, A), \delta_\bullet)$ associated to $g_1, \ldots, g_4$ over $A$ and denote $Z_i = \ker(\delta_i)$, $B_i = \operatorname{im}(\delta_{i+1})$. It is of the form

$$A(-4d) \xrightarrow{\delta_4} A(-3d)^4 \xrightarrow{\delta_3} A(-2d)^6 \xrightarrow{\delta_2} A(-d)^4 \xrightarrow{\delta_1} A$$

where the differentials are matrices with $\pm g_1, \ldots, \pm g_4$ as non-zero entries. We set $\mathcal{Z}_i = Z_i(i \cdot d) \otimes_A A[\underline{T}]$, which we will consider as bigraded $A[\underline{T}]$-modules (one grading is induced by the grading of $A$, the other one comes from setting $\deg(T_i) = 1$ for all $i$). Now the approximation complex of cycles $(\mathcal{Z}_\bullet(\underline{g}, A), \epsilon_\bullet)$, or simply $\mathcal{Z}_\bullet$, is the complex

$$0 \to \mathcal{Z}_3(-3) \xrightarrow{\epsilon_3} \mathcal{Z}_2(-2) \xrightarrow{\epsilon_2} \mathcal{Z}_1(-1) \xrightarrow{\epsilon_1} \mathcal{Z}_0$$

where the differentials $\epsilon_\bullet$ are obtained by replacing $g_i$ by $T_i$ for all $i$ in the matrices of $\delta_\bullet$ and where the degree shifts are with respect to the grading by the $T_i$. As in (31), $\operatorname{im}(\epsilon_1)$ is generated by the linear syzygies of the $g_i$ and

$$H_0(\mathcal{Z}_\bullet) = A[\underline{T}]/\operatorname{im}(\epsilon_1) \simeq \operatorname{Sym}_A(I)$$

From now on, when we take the degree $\nu$ part of the approximation complex, denoted $(\mathcal{Z}_\bullet)_\nu$, it should always be understood to be taken with respect to the grading of $A$. Hereafter we denote by $\mathfrak{m}$ the maximal ideal $(X_0, \ldots, X_m) \subset A$.

The geometric intuition behind the $\mathcal{Z}$-complex is quite profound, we only give some hints and refer to [**Ch06**, Sect. 3] or [**Va94**] for a more thorough treatment of the subject. The symmetric algebra is closely related to the Rees algebra $\mathrm{Rees}_A(I)$, which can be defined as the quotient of $A[\underline{T}]$ by all syzygies (not only the linear ones). One has thus a canonical surjection from $\mathrm{Sym}_A(I)$ onto $\mathrm{Rees}_A(I)$, which induces an inclusion

$$\mathrm{Biproj}(\mathrm{Rees}_A(I)) \hookrightarrow \mathrm{Biproj}(\mathrm{Sym}_A(I)) \tag{37}$$

Now $\mathrm{Biproj}(\mathrm{Rees}_A(I))$ corresponds to the closure of the graph of the map $\psi$ and its image by the projection to $\mathbb{P}^3$ equals the surface $\mathscr{S}$, while $\mathrm{Biproj}(\mathrm{Sym}_A(I))$ is a priori a bigger object. However, $\mathrm{Sym}_A(I)$ is in some ways easier to study and under suitable conditions on the base points the inclusion in (37) becomes an isomorphism and one can retrieve the information about $\mathscr{S}$ contained in the Rees algebra from the symmetric algebra. More precisely, we will see that the implicit equation of $\mathscr{S}$ can be obtained from the determinant of certain graded parts of the $\mathcal{Z}$-complex.

The next lemma shows that the complex $\mathcal{Z}_\bullet(g_1, \ldots, g_4; A)$ is acyclic if the base points are local complete intersections and finite in number. This is a standard hypothesis for syzygy-based implicitization methods, see [**KD06**].

Lemma 4.4. *If $I = (g_1, g_2, g_3, g_4) \subset A$ is of codimension 2 (i.e. if there are only finitely many base points) and if the base points $\mathscr{P} := \mathrm{Proj}(A/I) \subset \mathscr{T}$ form a local complete intersection, then the complex $\mathcal{Z}_\bullet$ is acyclic.*

Proof. This follows immediately from [**BJ03**, Prop. 4.9]. We only have to check that the hypotheses of that proposition are verified: In our case, we have $n = 4$ and we need to check that $\dim(A) = \mathrm{depth}_{\mathfrak{m}}(A) = n - 1 = 3$, which is true because $A$ is Cohen-Macaulay by Lemma 4.3 and because $A$ is the homogeneous coordinate ring of a (projective) surface. Moreover, $\mathrm{depth}_I(A) = \mathrm{codim}(I) = 2 = n - 2$ is again a consequence of the Cohen-Macaulayness of $A$. □

Remark 4.5. It can possibly be shown in a similar way as in Lemma 3.3 that the $\mathcal{Z}$-complex is still acyclic if the base points are almost local complete intersections, but we will not treat this case here.

**3.2. Bounds on local cohomology.** The following lemma establishes a vanishing criterion on the local cohomology of $\mathrm{Sym}_A(I)$, which

ensures that the implicit equation can be obtained as a generator of the annihilator of the symmetric algebra in a certain degree. We refer to the remark before Lemma 3.4 and to [**BS98**] for more details on local cohomology, a detailed treatment of which is beyond the scope of this work.

LEMMA 4.6. *Suppose that* $\mathscr{P} := \mathrm{Proj}(A/I) \subset \mathscr{T}$ *has dimension* 0 *and is locally a complete intersection. If* $\eta$ *is an integer such that*

$$H^0_{\mathfrak{m}}(\mathrm{Sym}_A(I))_\nu = 0 \quad \textit{for all } \nu \geq \eta$$

*then we have*

$$\mathrm{ann}_{\mathbb{K}[\underline{T}]}(\mathrm{Sym}_A(I)_\nu) = \mathrm{ann}_{\mathbb{K}[\underline{T}]}(\mathrm{Sym}_A(I)_\eta) = \ker(h)$$

*for all* $\nu \geq \eta$.

PROOF. The proof of Lemma 3.4 can be applied verbatim. □

As we shall see, the annihilator in the above lemma can be computed as the determinant (or MacRae invariant) of the complex $(\mathscr{Z}_\bullet)_\eta$, so we should give an explicit formula for the integer $\eta$. Like in Proposition 3.6, we first need to study the local cohomology of $A$ using its combinatorial structure as a semigroup ring. The following definition is the same as [**MS05**, Def. 11.15].

DEFINITION 4.7. Let $M$ be a graded $A$-module. The Matlis dual $M^\vee$ of $M$ is the $A$-module defined by

$$(M^\vee)_{-u} = \mathrm{Hom}_{\mathbb{K}}(M_u, \mathbb{K}),$$

the multiplication being the transpose. One has $(M^\vee)^\vee = M$ if all the graded parts $M_u$ of $M$ are finite-dimensional as $\mathbb{K}$-vector spaces.

LEMMA 4.8. *Let* $M$ *be a finitely generated graded* $A$*-module of dimension* $r$*. Then* $M$ *is Cohen-Macaulay if and only if* $H^i_{\mathfrak{m}}(M) = 0$ *for all* $i \neq r$ *and* $H^r_{\mathfrak{m}}(M) = \omega_M^\vee$ *is the Matlis dual to* $\omega_M$*.*

PROOF. This is [**MS05**, Th. 13.37]. □

So the local cohomology of an $A$-module that is Cohen-Macaulay can be expressed in terms of its canonical module. Let us apply this to the $A$-module $A$. Using that $\dim(A) = 3$ and that $A$ is Cohen-Macaulay by Lemma 4.3 we immediately deduce

COROLLARY 4.9. *The local cohomology of* $A$ *is*

$$H^i_{\mathfrak{m}}(A) = \begin{cases} 0 & \text{if } i \neq 3 \\ \omega_A^\vee & \text{if } i = 3 \end{cases}$$

*where* $\omega_A^\vee$ *is the Matlis dual to the canonical module* $\omega_A$*.*

So the third local cohomology module of $A$ is the only one that is non-zero. Actually, we do not need to know this module exactly; it is sufficient to know in which graded parts it vanishes.

COROLLARY 4.10. *Let $\nu \in \mathbb{Z}$. Then we have*

$$H^3_{\mathfrak{m}}(A)_\nu = 0 \qquad \text{if } \nu \geq 0$$

*Moreover, if $\mathrm{N}'(f)$ (or equivalently $C_1$) contains no interior point, then this bound can be lowered to $\nu \geq -1$, and if additionally the interior of $C_2$ is empty, it can be lowered to $\nu \geq -2$.*

PROOF. By Corollary 4.9 and the definition of the Matlis dual we have the following identities

$$\begin{aligned} H^3_{\mathfrak{m}}(A)_\nu &= (\omega_A^\vee)_\nu \\ &= \mathrm{Hom}_{\mathbb{K}}((\omega_A)_{-\nu}, \mathbb{K}) \end{aligned}$$

but by the third bullet point in Lemma 4.3, the module $\omega_A$ is generated by the elements in the interior of $C$, i.e. by elements of degree at least 1, so whenever $\nu \geq 0$, it follows $(\omega_A)_{-\nu} = 0$ and the modules in the above equation are all zero.

If there are no points in the interior of $C_1$, then $(\omega_A)_{-\nu} = 0$ also for $\nu = -1$. If furthermore $C_2$ has no interior points, $(\omega_A)_{-\nu} = 0$ for $\nu = -2$. □

With these results under our belt, we can proceed to investigate the 0th local cohomology of the symmetric algebra, as in Theorem 3.5. We give a proof that closely follows the corresponding theorems [**BJ03**, 5.5 and 5.10]. It is essentially the same as the one of Theorem 3.5, but we give more details and make explicit the constructions.

THEOREM 4.11. *If $\mathscr{P} := \mathrm{Proj}(A/I) \subset \mathscr{T}$ is a local complete intersection of dimension 0 then*

$$H^0_{\mathfrak{m}}(\mathrm{Sym}_A(I))_\nu = 0 \qquad \text{for all } \nu \geq 2d$$

*If the interior of $\mathrm{N}'(f) = C_1$ is empty, then this is true for all $\nu \geq 2d-1$ and if additionally $C_2$ has no interior point, the bound can be lowered to $2d-2$.*

PROOF. We consider the following diagram

$$\begin{array}{ccccccccc}
0 & \to & \mathcal{C}^0_{\mathfrak{m}}(\mathcal{Z}_3) & \to & \mathcal{C}^0_{\mathfrak{m}}(\mathcal{Z}_2) & \to & \mathcal{C}^0_{\mathfrak{m}}(\mathcal{Z}_1) & \to & \mathcal{C}^0_{\mathfrak{m}}(\mathcal{Z}_0) \to 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
0 & \to & \mathcal{C}^1_{\mathfrak{m}}(\mathcal{Z}_3) & \to & \mathcal{C}^1_{\mathfrak{m}}(\mathcal{Z}_2) & \to & \mathcal{C}^1_{\mathfrak{m}}(\mathcal{Z}_1) & \to & \mathcal{C}^1_{\mathfrak{m}}(\mathcal{Z}_0) \to 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
0 & \to & \mathcal{C}^2_{\mathfrak{m}}(\mathcal{Z}_3) & \to & \mathcal{C}^2_{\mathfrak{m}}(\mathcal{Z}_2) & \to & \mathcal{C}^2_{\mathfrak{m}}(\mathcal{Z}_1) & \to & \mathcal{C}^2_{\mathfrak{m}}(\mathcal{Z}_0) \to 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
0 & \to & \mathcal{C}^3_{\mathfrak{m}}(\mathcal{Z}_3) & \to & \mathcal{C}^3_{\mathfrak{m}}(\mathcal{Z}_2) & \to & \mathcal{C}^3_{\mathfrak{m}}(\mathcal{Z}_1) & \to & \mathcal{C}^3_{\mathfrak{m}}(\mathcal{Z}_0) \to 0
\end{array}$$

where the first row is the $\mathcal{Z}_\bullet$-complex and the columns are the corresponding Čech complexes as defined in Chapter 3. From the theory of spectral sequences we know iteration processes which lead to limits with isomorphic total complexes and, in particular, isomorphic main

diagonals. We will not explain this in detail, but the first iteration process starts by taking the cohomology first in the rows, then in the columns. All but the first column will vanish by the acyclicity of the $\mathcal{Z}_\bullet$-complex and by the exactness of the localization functor and the entry in the upper right corner will become $H^0_{\mathfrak{m}}(\mathrm{Sym}_A(I))$, which will also be the direct sum over the main diagonal in the limit, as the diagonal does not change in the rest of the iteration process. The other iteration process starts with computing the cohomology first with respect to the columns and in this case one obtains the local cohomology modules $H^i_{\mathfrak{m}}(\mathcal{Z}_i)$ on the main diagonal. If an entry of the diagram is zero, it will stay zero throughout the iteration, so at this point we can already conclude that if the $H^i_{\mathfrak{m}}(\mathcal{Z}_i)$ all vanish, so will the main diagonals of the limit diagrams, which in the first case will be $H^0_{\mathfrak{m}}(\mathrm{Sym}_A(I))$. So it is sufficient to show that $H^i_{\mathfrak{m}}(\mathcal{Z}_i)_\nu = 0$ for $\nu \geq 2d$ (resp. $2d-1$, if the interior of $\mathrm{N}'(f)$ is empty or $2d-2$ if the interior of both $\mathrm{N}'(f) = C_1$ and $C_2$ is empty).
It suffices to show that $H^i_{\mathfrak{m}}(Z_i)_\nu = 0$, because $\mathcal{Z}_i = Z_i(i \cdot d) \otimes_A A[T_1, \ldots, T_4]$. Now as $\mathrm{depth}_A(I) = 2$, the Koszul complex is exact for $i > 4-2 = 2$, i.e. $B_i = Z_i$. It is clear by construction of the Koszul complex that $Z_4 = 0$ and that $B_3 = \mathrm{im}(\delta_3) \simeq A(-d)$. Using the fact that $H^3_{\mathfrak{m}}(A)_\nu = 0$ for $\nu \geq 0$ (resp. $\nu \geq -1$ or $\nu \geq -2$) by Corollary 4.10 we can deduce that $H^3_{\mathfrak{m}}(Z_3)_\nu = H^3_{\mathfrak{m}}(B_3)_\nu = 0$ if $\nu \geq d$ (resp. $\nu \geq d-1$ or $\nu \geq d-2$). For $i \geq 2$ we have the exact sequences

$$0 \to B_{i+1}(-d) \to K_{i+1}(-d) \to B_i \to 0$$

which gives rise to the following segment of the long exact sequence of cohomology

$$H^i_{\mathfrak{m}}(K_{i+1}(-d)) \to H^i_{\mathfrak{m}}(B_i) \to H^{i+1}_{\mathfrak{m}}(B_{i+1}(-d))$$

Now for $i = 2$, $H^i_{\mathfrak{m}}(K_{i+1}(-d)) = 0$ by Corollary 4.10 because $K_3 = A(-3d)^4$ and for all $\nu \geq 2d$ (resp. $\nu \geq 2d-1$ or $\nu \geq 2d-2$) we have $H^3_{\mathfrak{m}}(B_3(-d))_\nu = 0$ by the above and therefore $H^2_{\mathfrak{m}}(B_2)_\nu = 0$ as well. Moreover, $H^2_{\mathfrak{m}}(Z_2/B_2) = 0$ as $Z_2/B_2$ is supported on $\mathscr{P}$ which is of dimension 0, so the long exact sequence of cohomology associated to

$$0 \to B_2 \to Z_2 \to Z_2/B_2 \to 0$$

shows that $H^2_{\mathfrak{m}}(Z_2)_\nu = 0$ in this case as well. Finally, the exact sequence $0 \to Z_1(-d) \to A(-d)^4 \to I \to 0$ gives the segment

$$H^0_{\mathfrak{m}}(I) \to H^1_{\mathfrak{m}}(Z_1(-d)) \to H^1_{\mathfrak{m}}(A(-d)^4)$$

Now $H^1_{\mathfrak{m}}(A(-d)^4) = H^1_{\mathfrak{m}}(A(-d))^4 = 0$ by Corollary 4.9 and $H^0_{\mathfrak{m}}(I) = \{x \in I \mid \mathfrak{m}^k x = 0 \text{ for some } k \geq 0\} = 0$ because $A$ is a domain, so we immediately deduce $H^1_{\mathfrak{m}}(Z_1)_\nu = 0$ for all $\nu \in \mathbb{Z}$.

□

REMARK 4.12. For bihomogeneous parametrizations as in Chapter 3 we obtain the same bound as in Theorem 3.5 without the correction term $\mathrm{indeg}(I^{\mathrm{sat}})$, i.e $2d-1$. Also, in the case of homogeneous parametrization, i.e. $\mathscr{T} = \mathbb{P}^2$, the bound $2d-2$ coincides with the known bound, see [**BJ03**, Prop. 5.10]. In the toric case, there are counterexamples where one cannot lower the bound by $\mathrm{indeg}(I^{\mathrm{sat}})$, see Example 4.19. It is true, however, that one can lower the bound when base points are present, but we do not know how to describe the optimal bound by an explicit formula.

## 4. The implicit equation

It can now be deduced that the implicit equation of $\mathscr{S}$ is the determinant of the $\mathcal{Z}_\bullet$-complex.

THEOREM 4.13. *Assume that* $\dim(\mathscr{P}) = 0$ *and that* $\mathscr{P}$ *is locally a complete intersection. Let* $\nu_0 = 2d$. *For any integer* $\nu \geq \nu_0$ *the determinant* $D$ *of the complex* $(\mathcal{Z}_\bullet)_\nu$ *of* $\mathbb{K}[\underline{T}]$*-modules defines (up to multiplication with a constant) the same non-zero element in* $\mathbb{K}[\underline{T}]$ *and*

$$D = F^{\deg(\psi)}$$

*where* $F$ *is the implicit equation of* $\mathscr{S}$. *If the interior of* $\mathrm{N}'(f) = C_1$ *is empty, the statement is also true for* $\nu_0 = 2d-1$ *and if additionally* $C_2$ *has no interior points, one may take* $\nu_0 = 2d-2$.

PROOF. The proof is analogous to the proof of [**BJ03**, Th. 5.2], using Lemma 4.4, Lemma 4.6, and Theorem 4.11. □

While we believe that as in Theorem 3.8 this result could possibly be generalized to the case of almost local completion intersection base points, the proof of that theorem (or the one of [**BC05**, Th. 4]) does not apply directly here, because it uses at some points that $A$ is Gorenstein, which is not the case in the toric setting.

By [**GKZ94**, Appendix A], the determinant $D$ can be computed either as an alternating sum of subdeterminants of the differentials in $\mathcal{Z}_\nu$ or as the greatest common divisor of the maximal-size minors of the matrix $M$ associated to the first map $(\mathcal{Z}_1)_\nu \to (\mathcal{Z}_0)_\nu$. This matrix can be computed with the same algorithm as in Section 3.4. As an immediate corollary we deduce

COROLLARY 4.14. *Let* $M$ *be the matrix of the first map* $(\mathcal{Z}_1)_\nu \to (\mathcal{Z}_0)_\nu$ *of the complex* $(\mathcal{Z}_\bullet)_\nu$. *Then* $M$ *is a representation matrix for the surface* $\mathscr{S}$.

## 5. The special case $\mathscr{T} = \mathbb{P}^1 \times \mathbb{P}^1$

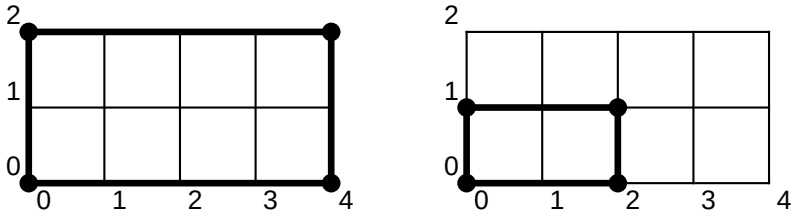
Bihomogeneous parametrizations, i.e. the case $\mathscr{T} = \mathbb{P}^1 \times \mathbb{P}^1$, are particularly important in practical applications, so we will now make explicit

the most important constructions in that case and make some refinements. We also include an implementation in Macaulay2 [**M2**] in the Appendix.

In this section, we consider a rational parametrization of a surface $\mathscr{S}$

$$\begin{array}{rcl} \mathbb{P}^1 \times \mathbb{P}^1 & \overset{\phi}{\dashrightarrow} & \mathbb{P}^3 \\ (s:u) \times (t:v) & \mapsto & (f_1 : f_2 : f_3 : f_4)(s,u,t,v) \end{array}$$

where the polynomials $f_1, \ldots, f_4$ are bihomogeneous of bidegree $(e_1, e_2)$ with respect to the homogeneous variable pairs $(s:u)$ and $(t:v)$, and $e_1, e_2$ are positive integers. We make the same assumptions as in the general toric case. Let $d = \gcd(e_1, e_2)$, $e_1' = \frac{e_1}{d}$, and $e_2' = \frac{e_2}{d}$. So we assume that the Newton polytope $\mathrm{N}(f)$ is a rectangle of length $e_1$ and width $e_2$ and $\mathrm{N}'(f)$ is a rectangle of length $e_1'$ and width $e_2'$ (in reality $\mathrm{N}(f)$ might be smaller, but in this section we homogenize with respect to the whole rectangle). This is illustrated in the following diagram for $e_1 = 4$ and $e_2 = 2$.




$\mathrm{N}(f)$ $\qquad$ $\mathrm{N}'(f)$

So $\mathbb{P}^1 \times \mathbb{P}^1$ can be embedded in $\mathbb{P}^m$, $m = (e_1' + 1)(e_2' + 1) - 1$ through the *Segre-Veronese embedding* $\rho = \rho_{e_1,e_2}$

$$\begin{array}{rcl} \mathbb{P}^1 \times \mathbb{P}^1 & \overset{\rho}{\dashrightarrow} & \mathbb{P}^m \\ (s:u) \times (t:v) & \mapsto & (\ldots : s^i u^{e_1'-i} t^j v^{e_2'-j} : \ldots) \end{array}$$

We denote by $\mathscr{T}$ its image, which is an irreducible surface of degree 2 in $\mathbb{P}^m$, whose ideal $J$ is generated by quadratic binomials. We have the following commutative diagram.

(38)
$$\begin{array}{ccc} \mathbb{P}^1 \times \mathbb{P}^1 & \overset{\phi}{\dashrightarrow} & \mathbb{P}^3 \\ \downarrow \rho & \nearrow_{\psi} & \\ \mathscr{T} & & \end{array}$$

with $\psi = (g_1 : \ldots : g_4)$, the $g_i$ being polynomials in the variables $X_0, \ldots, X_m$ of degree $d$. We denote by $A = \mathbb{K}[X_0, \ldots, X_m]/J$ the

homogeneous coordinate ring of $\mathscr{T}$. We can give an alternative construction of the coordinate ring; consider the $\mathbb{N}$-graded $\mathbb{K}$-algebra

$$S := \bigoplus_{n\in\mathbb{N}} \left(\mathbb{K}[s,u]_{ne_1'} \otimes_{\mathbb{K}} \mathbb{K}[t,v]_{ne_2'}\right) \subset \mathbb{K}[s,u,t,v]$$

which is finitely generated by $S_1$ as an $S_0$-algebra. Then $\mathbb{P}^1 \times \mathbb{P}^1$ is the bihomogeneous spectrum $\mathrm{Biproj}(S)$ of $S$, since $\mathrm{Proj}(\bigoplus_{n\in\mathbb{N}} \mathbb{K}[s,u]_{ne_1'}) = \mathrm{Proj}(\bigoplus_{n\in\mathbb{N}} \mathbb{K}[t,v]_{ne_2'}) = \mathbb{P}^1$. The Segre-Veronese embedding $\rho$ induces an isomorphism of $\mathbb{N}$-graded $\mathbb{K}$-algebras

$$\begin{array}{rcl} A & \stackrel{\theta}{\to} & S \\ X^{i,j} & \mapsto & s^i u^{e_1'-i} t^j v^{e_2'-j} \end{array}$$

where $X^{i,j} = X_{(e_2'+1)i+j}$ for $i = 0,\ldots,e_1'$ and $j = 0,\ldots,e_2'$ and the implicit equation of $\mathscr{S}$ can be obtained by the method of approximation complexes described in the previous sections as the kernel of the map

$$\begin{array}{rcl} \mathbb{K}[T_1,\ldots,T_4] & \to & A \\ T_i & \mapsto & g_i \end{array}$$

By Lemma 4.3, $A$ is an affine normal semigroup ring and it is Cohen-Macaulay. It is Gorenstein if and only if $e_1' = e_2' = 1$ (or equivalently $e_1 = e_2$), which is the case treated in Chapter 3. The ideal $J$ is easier to describe than in the general toric case (compare [**Su06**, 6.2] for the case $e_2' = 2$):

LEMMA 4.15. *The generators of $J$ can be described explicitly: Let*

$$A_i = \begin{pmatrix} X^{i,0} & \ldots & X^{i,e_2'-1} \\ X^{i,1} & \ldots & X^{i,e_2'} \end{pmatrix},$$

*then the 2-minors of the matrix*

$$\begin{pmatrix} A_0 & \ldots & A_{e_1'-1} \\ A_1 & \ldots & A_{e_1'} \end{pmatrix}$$

*generate the ideal $J$.*

Let us also state the degree formula for this setting, which is a direct corollary of Proposition 4.2.

PROPOSITION 4.16.

$$\deg(\psi)\deg(\mathscr{S}) = 2e_1e_2 - \sum_{\mathfrak{p}\in V(g_1,\ldots,g_4)\subset\mathscr{T}} e_{\mathfrak{p}}$$

*where $e_{\mathfrak{p}}$ is the multiplicity of the base point $\mathfrak{p}$.*

We have claimed before that it is better to choose the toric variety defined by $\mathrm{N}'(f)$ instead of $\mathrm{N}(f)$. Let us now give some explanations why this is the case. As we have seen, a bihomogeneous parametrization of bidegree $(e_1,e_2)$ gives rise to the toric variety $\mathscr{T} = \mathbb{P}^1\times\mathbb{P}^1$ determined

by a rectangle of length $e_1'$ and width $e_2'$, where $e_i' = \frac{e_i}{d}$, $d = \gcd(e_1, e_2)$, and whose coordinate ring can be described as

$$S := \bigoplus_{n\in\mathbb{N}} \left(\mathbb{K}[s,u]_{ne_1'} \otimes_{\mathbb{K}} \mathbb{K}[t,v]_{ne_2'}\right) \subset \mathbb{K}[s,u,t,v]$$

Instead of this embedding of $\mathbb{P}^1 \times \mathbb{P}^1$ we could equally choose the embedding defined by $\mathrm{N}(f)$, i.e. a rectangle of length $e_1$ and width $e_2$, in which case we obtain the following coordinate ring

$$\hat{S} := \bigoplus_{n\in\mathbb{N}} \left(\mathbb{K}[s,u]_{ne_1} \otimes_{\mathbb{K}} \mathbb{K}[t,v]_{ne_2}\right) \subset \mathbb{K}[s,u,t,v]$$

It is clear that this ring also defines $\mathbb{P}^1 \times \mathbb{P}^1$ and we obviously have an isomorphism

$$\hat{S}_n \simeq S_{d\cdot n}$$

between the graded parts of the two rings, which means that the grading of $\hat{S}$ is coarser and contains less information. It is easy to check that the above isomorphism induces an isomorphism between the corresponding graded parts of the approximation complexes $\mathcal{Z}_\bullet$ corresponding to $S$ and $\hat{\mathcal{Z}}_\bullet$ corresponding to $\hat{S}$, namely

$$\hat{\mathcal{Z}}_\nu \simeq \mathcal{Z}_{d\cdot\nu}$$

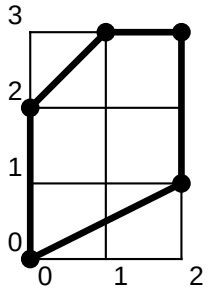
If the optimal bound in Theorem 4.13 for the complex $\mathcal{Z}$ is a multiple of $d$, i.e. $\nu_0 = d \cdot \eta$, then the optimal bound for $\hat{\mathcal{Z}}$ is $\hat{\nu}_0 = \eta$ and we obtain isomorphic complexes in these degrees and the matrix sizes will be equal in both cases. If not, the optimal bound $\hat{\nu}_0$ is the smallest integer bigger than $\frac{\nu_0}{d}$ and in this case, the vector spaces in $\hat{\mathcal{Z}}_{\hat{\nu}_0}$ will be of higher dimension than their counterparts in $\mathcal{Z}_{\nu_0}$ and the matrices of the maps will be bigger. An example of this is given in the next section.

## 6. Examples and final remarks

Example 4.17. We first treat some examples from [**KD06**]. Example 10 in the cited paper, which we failed to solve in a satisfactory manner in Section 3.5, is a surface parametrized by

$$\begin{aligned}
f_1 &= (t+t^2)(s-1)^2 + (1+st-s^2t)(t-1)^2 \\
f_2 &= (-t-t^2)(s-1)^2 + (-1+st+s^2t)(t-1)^2 \\
f_3 &= (t-t^2)(s-1)^2 + (-1-st+s^2t)(t-1)^2 \\
f_4 &= (t+t^2)(s-1)^2 + (-1-st-s^2t)(t-1)^2
\end{aligned}$$

The Newton polytope $\mathrm{N}'(f)$ of this parametrization is




We can compute the new parametrization over the associated variety, which is given by linear forms $g_1, \ldots, g_4$, i.e. $d = 1$ (since there is no smaller homothety $\mathrm{N}'(f)$ of $\mathrm{N}(f)$) and the coordinate ring is $A = \mathbb{K}[X_0, \ldots, X_8]/J$ where $J$ is generated by 21 binomials of degrees 2 and 3. Recall that the 9 variables correspond to the 9 points in the Newton polytope. The expected degree bound of the $\mathscr{Z}_\bullet$ is $2 \cdot 1 = 2$, but it turns out that it can actually be lowered to $\nu_0 = 1$, as there is a LCI base point. In this degree, the implicit equation of degree 5 of the surface $\mathscr{S}$ is represented by a $9 \times 14$-matrix, compared to a $15 \times 15$-matrix with the toric resultant method (from which a $11 \times 11$-minor has to be computed) and a $5 \times 5$-matrix with the method of moving planes and quadrics. Note also that this is a major improvement of the method of Chapter 3, where we obtained a $42 \times 36$-matrix representation for the same example.

Example 4.18. Example 11 of [**KD06**] is similar to Example 10 but an additional term is added, which transforms the point $(1, 1)$ into a non-LCI base point. The parametrization is

$$\begin{aligned}
f_1 &= (t+t^2)(s-1)^2 + (1+st-s^2t)(t-1)^2 + (t+st+st^2)(s-1)(t-1)\\
f_2 &= (-t-t^2)(s-1)^2 + (-1+st+s^2t)(t-1)^2 + (t+st+st^2)(s-1)(t-1)\\
f_3 &= (t-t^2)(s-1)^2 + (-1-st+s^2t)(t-1)^2 + (t+st+st^2)(s-1)(t-1)\\
f_4 &= (t+t^2)(s-1)^2 + (-1-st-s^2t)(t-1)^2 + (t+st+st^2)(s-1)(t-1)
\end{aligned}$$

The Newton polytope has not changed, so the embedding as a toric variety and the coordinate ring $A$ are the same as in the previous example. Again the new map is given by $g_1, \ldots, g_4$ of degree 1.

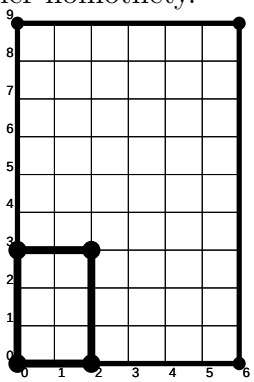
As in [**KD06**], the method represents (with $\nu_0 = 1$) the implicit equation of degree 5 times a linear extraneous factor caused by the non-LCI base point. While the Chow form method represents this polynomial as a $12 \times 12$-minor of a $15 \times 15$-matrix, our representation matrix is $9 \times 13$. Note that in this case, the method of moving lines and quadrics fails.

Example 4.19. In this example, we will see that if the ring $A$ is not Gorenstein, one cannot always lower the bound $\nu_0$ by the initial degree

of the saturation of $I$, as in Chapter 3. Consider the parametrization

$$\begin{aligned} f_1 &= (s^2+t^2)t^6s^4 + (1+s^3t^4-s^4t^4)(t-1)^5(s^2-1) \\ f_2 &= (-s^2-t^2)t^6s^4 + (-1+s^3t^4+s^4t^4)(t-1)^5(s^2-1) \\ f_3 &= (s^2-t^2)t^6s^4 + (-1-s^3t^4+s^4t^4)(t-1)^5(s^2-1) \\ f_4 &= (s^2+t^2)t^6s^4 + (-1-s^3t^4-s^4t^4)(t-1)^5(s^2-1) \end{aligned}$$

We will consider this as a bihomogeneous parametrization of bidegree $(6,9)$, that is we will choose the embedding $\rho$ corresponding to the smaller rectangle in the following picture (of length 2 and width 3). The actual Newton polytope $\mathrm{N}(f)$ is smaller than the big rectangle, but does not allow a smaller homothety.




Here $A = \mathbb{K}[X_0, \ldots, X_{11}]/J$, where $J$ is generated by 43 quadratic binomials and the associated $g_i$ are of degree $d = 3$. It turns out that $\nu_0 = 4$ is the lowest degree such that the implicit equation of degree 46 is represented as determinant of $\mathcal{Z}_{\nu_0}$, the matrix of the first map being of size $117 \times 200$. So we cannot compute $\nu_0$ as $2d - \mathrm{indeg}(I^{\mathrm{sat}}) = 6 - 3 = 3$, as one might have thought. This is of course due to $A$ not being Gorenstein, since the rectangle contains two interior points.

Let us make a remark on the complexity of the computation of the representation matrix. It turns out that this is highly efficient. Even if we choose the non-optimal bound $\nu = 6$ as given in Theorem 4.13, the computation of the $247 \times 518$ representation matrix is computed instantaneously in Macaulay2. Just to give an idea of what happens if we take higher degrees: For $\nu = 30$ a $5551 \times 15566$-matrix is computed in about 30 seconds, and for $\nu = 50$ we need slightly less than 5 minutes to compute a $15251 \times 43946$ matrix.

In any case, the computation of the matrix is relatively cheap and the main interest in lowering the bound $\nu_0$ as much as possible is the reduction of the size of the matrix, not the time of its computation.

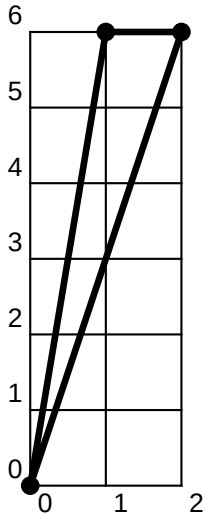
Example 4.20. In the previous example, we did not fully exploit the structure of $\mathrm{N}(f)$ and chose a bigger polygon for the embedding. Here is an example where this is necessary to represent the implicit equation

without extraneous factors.

$$\begin{aligned} f_1 &= st^6 + 2 \\ f_2 &= st^5 - 3st^3 \\ f_3 &= st^4 + 5s^2t^6 \\ f_4 &= 2 + s^2t^6 \end{aligned}$$

This is a very sparse parametrization and we have $\mathrm{N}(f) = \mathrm{N}'(f)$. The coordinate ring is $A = \mathbb{K}[X_0, \ldots, X_5]/J$, where $J = (X_3^2 - X_2X_4, X_2X_3 - X_1X_4, X_2^2 - X_1X_3, X_1^2 - X_0X_5)$ and the new base-point-free parametrization $\psi$ is given by

$$(g_1, g_2, g_3, g_4) = (2X_0 + X_4, -3X_1 + X_3, X_2 + 5X_5, 2X_0 + X_5)$$




$\mathrm{N}(f)$

For $\nu_0 = 2d = 2$ we can compute the matrix of the first map of $(\mathcal{Z}_\bullet)_{\nu_0}$, which is a $17 \times 34$-matrix. The greatest common divisor of the 17-minors of this matrix is the homogeneous implicit equation of the surface; it is of degree 6 in the variables $T_1, \ldots, T_4$:

$$\begin{aligned} &2809T_1^2T_2^4 + 124002T_2^6 - 5618T_1^3T_2^2T_3 + 66816T_1T_2^4T_3 + 2809T_1^4T_3^2 \\ &-50580T_1^2T_2^2T_3^2 + 86976T_2^4T_3^2 + 212T_1^3T_3^3 - 14210T_1T_2^2T_3^3 + 3078T_1^2T_3^4 \\ &+13632T_2^2T_3^4 + 116T_1T_3^5 + 841T_3^6 + 14045T_1^3T_2^2T_4 - 169849T_1T_2^4T_4 \\ &-14045T_1^4T_3T_4 + 261327T_1^2T_2^2T_3T_4 - 468288T_2^4T_3T_4 - 7208T_1^3T_3^2T_4 \\ &+157155T_1T_2^2T_3^3T_4 - 31098T_1^2T_3^3T_4 - 129215T_2^2T_3^3T_4 - 4528T_1T_3^4T_4 \\ &-12673T_3^5T_4 - 16695T_1^2T_2^2T_4^2 + 169600T_2^4T_4^2 + 30740T_1^3T_3T_4^2 \\ &-433384T_1T_2^2T_3T_4^2 + 82434T_1^2T_3^2T_4^2 + 269745T_2^2T_3^2T_4^2 + 36696T_1T_3^3T_4^2 \\ &+63946T_3^4T_4^2 + 2775T_1T_2^2T_4^3 - 19470T_1^2T_3T_4^3 + 177675T_2^2T_3T_4^3 \\ &-85360T_1T_3^2T_4^3 - 109490T_3^3T_4^3 - 125T_2^2T_4^4 + 2900T_1T_3T_4^4 \\ &+7325T_3^2T_4^4 - 125T_3T_4^5 \end{aligned}$$

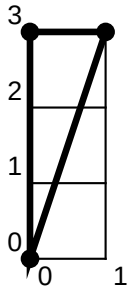
As in Example 4.19 we could have considered the parametrization as a bihomogeneous map either of bidegree $(2,6)$ or of bidegree $(1,3)$, i.e. we could have chosen the corresponding rectangles instead of $\mathrm{N}(f)$. This leads to more complicated coordinate rings (20 resp. 7 variables and 160 resp. 15 generators of $J$) and to bigger matrices (of size $21\times 34$ in both cases). Even more importantly, the parametrizations will have a non-LCI base point and the matrices do not represent the implicit equation but a multiple of it (of degree 9).

In other words, in this example the toric version of the method of approximation complexes gives a significantly better result than the bihomogeneous version and - for similar reasons - the homogeneous version of the method.

Interestingly, we can even do better than with $\mathrm{N}(f)$ by choosing a smaller polytope. The philosophy is that the choice of the optimal polytope is a compromise between two criteria:

- The polytope should be as simple as possible in order to avoid that the ring $A$ becomes too complicated.
- The polytope should respect the sparseness of the parametrization (i.e. be close to the Newton polytope) so that no base points appear which are not local complete intersections.

So let us repeat the same example with another polytope $Q$, which is small enough to reduce the size of the matrix but which only adds well-behaved (i.e. local complete intersection) base points:




The Newton polytope $\mathrm{N}(f)$ is contained in $2\cdot Q$, so the parametrization will factor through the toric variety associated to $Q$, more precisely we obtain a new parametrization defined by

$$(g_1,g_2,g_3,g_4)=(2X_0^2+X_3X_4,-3X_0X_4+X_2X_4X_1X_4+5X_4^2,2X_0^2+X_4^2)$$

over the coordinate ring $A=\mathbb{K}[X_0,\ldots,X_4]/J$ with $J=(X_2^2-X_1X_3,$ $X_1X_2-X_0X_3,X_1^2-X_0X_2)$. The optimal bound is $\nu_0=2$ and in this degree the implicit equation is represented directly without extraneous factors by a $12\times 19$-matrix, which is smaller than the $17\times 34$ we had before.

**Final remarks.** In conclusion, we have extended the method of approximation complexes to the toric case (and as a special case to bihomogeneous parametrizations). This generalization provides a better understanding of the method through the use of combinatorial commutative algebra. From a practical point of view, it is also a major improvement, as it makes the method applicable for a much wider range of parametrizations (for example, by avoiding unnecessary base points with bad properties) and leads to significantly smaller representation matrices. Let us sum up the advantages and disadvantages compared to other techniques to compute matrix representations (e.g. the ones introduced in [**KD06**]). The most important advantages are:

- The method works in a very general setting and makes only minimal assumptions on the parametrization. In particular, it works well in the presence of base points.
- Only linear syzygies are used to construct the representation matrix, which means that the matrix can be very efficiently computed by solving a linear system.
- Unlike the method of toric resultants, we do not have to extract a maximal minor of unknown size, since the matrices are generically of full rank.
- The structure of the Newton polytope of the parametrization is respected and thus gives much better results for sparse parametrizations, both in terms of computation time and in terms of the size of the representation matrix. Moreover, it subsumes the known method of approximation complexes in the case of dense homogeneous parametrization, in which case the methods coincide.

Disadvantages of the method are the following.

- Unlike with the toric resultant or the method of moving planes and surfaces, the matrix representations are not square.
- The matrices involved are generally bigger than with the method of moving planes and surfaces.

It is important to remark that those disadvantages are inherent to the choice of the method: A square matrix built from linear syzygies does not exist in general and it is an automatic consequence that if one only uses linear syzygies to construct the matrix, it has to be bigger than a matrix which also uses entries of higher degree. The choice of the method to use depends very much on the given parametrization and on what one wants to do with the matrix representation.

As a last comment, we would like to mention that it in certain cases the methods will yield better results if one reparametrizes the surface before computing the representation matrix. This is further explained in the Appendix.

# Appendix - Implementations and examples

## A guided example for Chapter 4

In this appendix we show how to compute a matrix representation with the method developed in Chapter 4, using the computer algebra system Macaulay2 [**M2**]. For didactical reason and because it is probably the most interesting case from a practical point of view, we restrict our computations to bi-homogeneous parametrizations of a certain bidegree $(e_1, e_2)$. However, the method is easily adaptable to the toric case, or more precisely to a given fixed Newton polytope $\mathrm{N}(f)$ and, where it is appropriate, we will give hints on what to change in the code. Moreover, we are not claiming that our implementation is optimized for efficiency; anyone trying to implement the method to solve computationally involved examples is well-advised to give more ample consideration to this issue. For example, in the toric case there are better suited software systems to compute the generators of the toric ideal $J$, see [**4ti2**].

Let us start by defining the parametrization $\phi$ given by $(f_1, \ldots, f_4)$.

```
S=QQ[s,u,t,v];
e1=4;
e2=2;
f1=s^4*t^2+2*s*u^3*v^2
f2=s^2*u^2*t*v-3*u^4*t*v
f3=s*u^3*t*v+5*s^4*t^2
f4=2*s*u^3*v^2+s^2*u^2*t*v
F=matrix{{f1,f2,f3,f4}}
```

The reader can experiment with the implementation simply by changing the definition of the polynomials and their degrees, the rest of the code being identical.

We first set up the list $st$ of monomials $s^i t^j$ of bidegree $(e_1', e_2')$. In the toric case, this list should only contain the monomials corresponding to points in the Newton polytope $\mathrm{N}'(f)$.

```
st={};
l=-1;
d=gcd(e1,e2)
ee1=numerator(e1/d);
ee2=numerator(e2/d);
```

```
for i from 0 to ee1 do (
   for j from 0 to ee2 do (
   st=append(st,s^i*u^(ee1-i)*t^j*v^(ee2-j));
   l=l+1
   )
)
```

We compute the ideal $J$ and the quotient ring $A$. This is done by a Gröbner basis computation which works well for examples of small degree, but which should be replaced by the matrix formula in Lemma 4.15 for more complicated examples. In the toric case, there exist specialized software systems such as [**4ti2**] to compute the ideal $J$.

```
SX=QQ[s,u,t,v,w,x_0..x_l,MonomialOrder=>Eliminate 5]

X={};
st=matrix {st};
F=sub(F,SX)
st=sub(st,SX)

te=1;
for i from 0 to l do ( te=te*x_i )

J=ideal(1-w*te)
for i from 0 to l do (
    J=J+ideal (x_i - st_(0,i))
    )
J= selectInSubring(1,gens gb J)

R=QQ[x_0..x_l]
J=sub(J,R)
A=R/ideal(J)
```

Next, we set up the list $ST$ of monomials $s^i t^j$ of bidegree $(e_1, e_2)$ and the list $X$ of the corresponding elements of the quotient ring $A$. In the toric case, this list should only contain the monomials corresponding to points in the Newton polytope $\mathrm{N}(f)$.

```
use SX
ST={};
for i from 0 to e1 do (
    for j from 0 to e2 do (
    ST=append(ST,s^i*u^(e1-i)*t^j*v^(e2-j));
    )
)

X={};
for z from 0 to length(ST)-1 do (
```

```
    f=ST_z;
    xx=1;
    is=degree substitute(f,{u=>1,v=>1,t=>1});
    is=is_0;
    it=degree substitute(f,{u=>1,v=>1,s=>1});
    it=it_0;
    iu=degree substitute(f,{t=>1,v=>1,s=>1});
    iu=iu_0;
    iv=degree substitute(f,{u=>1,t=>1,s=>1});
    iv=iv_0;
    ded=0;
  while ded < k do (
     for mm from 0 to l do (
        js=degree substitute(st_(0,mm),{u=>1,v=>1,t=>1});
        js=js_0;
        jt=degree substitute(st_(0,mm),{u=>1,v=>1,s=>1});
        jt=jt_0;
        ju=degree substitute(st_(0,mm),{t=>1,v=>1,s=>1});
        ju=ju_0;
        jv=degree substitute(st_(0,mm),{u=>1,t=>1,s=>1});
        jv=jv_0;
if is>=js and it>=jt and iu>=ju and iv>=jv then (
    xx=xx*x_mm;
    ded=ded+1;
    is=is-js;
    it=it-jt;
    iv=iv-jv;
    iu=iu-ju; )));
   X=append(X,xx); )
```

We can now define the new parametrization $\psi$ by the polynomials $g_1, \ldots, g_4$.

```
X=matrix {X};
X=sub(X,SX)
(M,C)=coefficients(F,Variables=>
          {s_SX,u_SX,t_SX,v_SX},Monomials=>ST)
G=X*C
G=matrix{{G_(0,0),G_(0,1),G_(0,2),G_(0,3)}}
G=sub(G,A)
```

In the following, we construct the matrix representation $M$. For simplicity, we compute the whole module $\mathcal{Z}_1$, which is not necessary as we only need the graded part $(\mathcal{Z}_1)_{\nu_0}$. In complicated examples, one should compute only this graded part by directly solving the linear system described in Section 3.4. Remark that the best bound $nu = \nu_0$ depends on the parametrization.

```
use A
Z1=kernel koszul(1,G);
nu=2*d-1
S=A[T1,T2,T3,T4]
G=sub(G,S);
Z1nu=super basis(nu+d,Z1);
Tnu=matrix{{T1,T2,T3,T4}}*substitute(Z1nu,S);

lll=matrix {{x_0..x_l}}
lll=sub(lll,S)
ll={}
for i from 0 to l do { ll=append(ll,lll_(0,i)) }
(m,M)=coefficients(Tnu,Variables=>
          ll,Monomials=>substitute(basis(nu,A),S));
M;
```

The matrix $M$ is the desired matrix representation of the surface $\mathscr{S}$.

**Some useful commands to experiment with simple examples.** We close this appendix by indicating some easy ways to compute some interesting data, which can give additional insights when experimenting with examples. Note that what follows is rather expensive computationally and only works in small degrees. First, we can compute the whole $\mathscr{Z}$-complex.

```
use A
Z0=A^1;
Z1=kernel koszul(1,G);
Z2=kernel koszul(2,G);
Z3=kernel koszul(3,G);
```

The dimension of the vector spaces in the complex $\mathscr{Z}_\nu$ (or in any other degree) can then be obtained as follows.

```
hilbertFunction(nu,Z0)
hilbertFunction(nu+d,Z1)
hilbertFunction(nu+2*d,Z2)
hilbertFunction(nu+3*d,Z3)
```

The vanishing of the Euler characteristic is a necessary condition for the determinant of the complex representing the implicit equation. We can check this by the following command.

```
hilbertFunction(nu,Z0)-hilbertFunction(nu+d,Z1)
  +hilbertFunction(nu+2*d,Z2)-hilbertFunction(nu+3*d,Z3)
```

As we have seen in the proof of Theorem 3.8, the degree of the surface (or more precisely the degree of the surface times the degree of the parametrization) can be computed as the following alternating sum:

```
hilbertFunction(nu+d,Z1)-2*hilbertFunction(nu+2*d,Z2)
  +3*hilbertFunction(nu+3*d,Z3)
```

### Surface reparametrization as a preconditioning step

As we have seen, the size of the matrix representation depends on the given parametrization and in general it is advantageous to choose a simpler parametrization of the same surface, if that is possible. For example, approaches such as [**Sc03**] can be used to find a simpler reparametrization of the given surface and optimize the presented methods.

Another important factor to consider is that all the methods we have seen represent the implicit equation to the power of the degree of the parametrization. On the one hand, it can be seen as an advantage that this piece of geometric information is encoded in the matrix representation, but on the other hand, for certain applications one might be willing to sacrifice the information about the parametric degree in order to obtain smaller matrices. If this is the case, there exist (for certain surface parametrizations) algorithms to compute a proper reparametrization of the surface, see [**Pe06**] or [**LG06**] or Section 1.5, and in these cases it is highly advisable to do so before computing the matrix representation, because this will allow us to represent the implicit equation directly instead of one of its powers, and the matrices will be significantly smaller. Let us illustrate this with Example 2 from [**Pe06**], which treats a parametrization $\phi$ defined by

$$\begin{aligned} f_1 &= (s^4t^4 + 2s^4t^2 + 5s^4 + 2t^4 + 4t^2 + 11)(s^4 + 1) \\ f_2 &= (s^4t^4 + 2s^4t^2 + 5s^4 + t^4 + 2t^2 + 6) \\ f_3 &= -(s^4t^4 + 2s^4t^2 + 5s^4 + t^4 + 2t^2 + 3)(s^4 + 1) \\ f_4 &= (t^4 + 2t^2 + 5)(s^4 + 1) \end{aligned}$$

This is a parametrization of bidegree $(8, 4)$ and its Newton polytope is the whole rectangle of length 8 and width 4, so we can apply the method of approximation complexes for $\mathbb{P}^1 \times \mathbb{P}^1$. We obtain a matrix of size $45 \times 59$ representing $F_{\mathscr{S}}^{16}$, where

$$F_{\mathscr{S}} = 2T_1T_2 - T_2T_3 - 3T_1T_4 - 2T_2T_4 + 3T_4^2$$

is the implicit equation and $\deg(\phi) = 16$. Using the algorithm presented in [**Pe06**] one can compute the following proper reparametrization of the surface $\mathscr{S}$:

$$\begin{aligned} f_1 &= -(11 + st - 5s - 2t)(s - 1) \\ f_2 &= 6 - t - 5s + st \\ f_3 &= (-t + st - 5s + 3)(s - 1) \\ f_4 &= (t - 5)(s - 1) \end{aligned}$$

This parametrization of bidegree $(2, 1)$ represents $F_{\mathscr{S}}$ directly by the following $6 \times 11$-matrix.

$$\begin{pmatrix}
0 & 3T_1 - 5T_2 + T_3 & 0 & -3T_1 + 8T_2 & 0 & -3T_2 \\
-66T_1 + 121T_2 & 11T_1 - 22T_2 & -41T_1 & 5T_1 + T_2 & 50T_1 - 121T_2 + 50T_3 & -10T_1 + 21T_2 - 10T_3 - 6T_4 \\
0 & 0 & 3T_1 + 11T_3 & 5T_1 - 10T_2 & -5T_1 - 5T_3 & T_1 + 10T_2 + T_3 - 6T_4 \\
0 & 0 & -48T_1 + 88T_2 & 8T_1 - 16T_2 & 25T_1 - 88T_2 + 25T_3 & -5T_1 + 16T_2 - 5T_3 - 3T_4 \\
0 & 0 & 0 & 3T_1 - 5T_2 + T_3 & 0 & 5T_2 - 3T_4 \\
33T_1 + 121T_3 & 55T_1 - 110T_2 & -40T_1 & -63T_1 + 181T_2 & -25T_1 - 25T_3 & 5T_1 - 71T_2 + 5T_3 + 3T_4 \\
0 & 0 & 0 & 0 & -5T_1 - 5T_3 + 8T_4 & T_1 + T_3 - T_4 \\
0 & 0 & 0 & -T_1 + T_2 + T_4 & 0 & -T_2 \\
0 & 0 & -40T_1 + 88T_4 & -8T_1 + 16T_2 & -25T_1 - 25T_3 & 5T_1 - 16T_2 + 5T_3 + 3T_4 \\
0 & -T_1 + T_2 + T_4 & 0 & -T_2 & 0 & 0 \\
-440T_1 + 968T_4 & -88T_1 + 176T_2 & -200T_1 & 48T_1 - 184T_2 & -125T_1 - 125T_3 & 25T_1 + 8T_2 + 25T_3 + 15T_4
\end{pmatrix}$$

# Bibliography


[4ti2] 4ti2—A software package for algebraic, geometric and combinatorial problems on linear spaces, 4ti2 team, available at www.4ti2.de

[AHW05] W. A. Adkins, J. W. Hoffman, and H. H. Wang. Equations of parametric surfaces with base points via syzygies. *J. Symbolic Comput.*, 39(1):73–101, 2005.

[ACGS07] D. A. Aruliah and Robert M. Corless and Laureano Gonzalez-Vega and Azar Shakoori, Geometric applications of the Bezout matrix in the Lagrange basis, SNC '07: Proceedings of the 2007 International Workshop on Symbolic-Numeric Computation, London, Ontario, Canada. 2007, pp. 55–64.

[BS98] Brodmann, M. P. and Sharp, R. Y., Local cohomology: an algebraic introduction with geometric applications, Cambridge Studies in Advanced Mathematics 60, Cambridge University Press, 1998.

[BH93] W. Bruns and J. Herzog. *Cohen-Macaulay rings*, volume 39 of *Cambridge Studies in Advanced Mathematics*. First edition. Cambridge University Press, Cambridge, 1993.

[BC05] Busé, L., Chardin, M., 2005. Implicitizing rational hypersurfaces using approximation complexes. J. Symbolic Comput. 40 (4-5), 1150–1168.

[BCJ06] Busé, L., Chardin, M., Jouanolou, J.-P., Torsion of the symmetric algebra and implicitization, 2006, to appear, preprint available at http://arxiv.org/abs/math/0610186.

[BCD03] L. Busé, D. Cox, and C. D'Andrea. Implicitization of surfaces in $\mathbb{P}^3$ in the presence of base points. *J. Algebra Appl.*, 2(2):189–214, 2003.

[BD07] L. Busé and M. Dohm. Implicitization of Bihomogeneous Parametrizations of Algebraic Surfaces via Linear Syzygies. *Proceedings of the International Symposium on Symbolic and Algebraic Computation (ISSAC 2007)*, p. 69-76, 2007.

[BJ03] L. Busé and J.-P. Jouanolou. On the closed image of a rational map and the implicitization problem. *J. Algebra*, 265(1):312–357, 2003.

[BEG07] Busé, L., Elkadi, M., and Galligo, A., 2007. A computational study of ruled surfaces, accepted to appear in *J. Symbolic Comput.*

[BKM05] L.Busé, H. Khalil, B. Mourrain. Resultant-based methods for plane curves intersection problems, Proceedings of the CASC'2005 conference, Lecture Notes in Computer Science, Vol. 3718 (2005), pp. 75-92.

[Ce92] T.E. Cecil, Lie Sphere Geometry, Springer, 1992.

[Ch00] Chardin, Marc. Applications of some properties of the canonical module in computational projective algebraic geometry. Symbolic computation in algebra, analysis, and geometry. J. Symbolic Comput. 29, 2000, 4-5, pp. 527–544.

[Ch06] Chardin, Marc. Implicitization using approximation complexes, Algebraic geometry and geometric modeling, Math. Vis., pp. 23–35, Springer, Berlin, 2006.

[Ch03] F.Chen, Reparametrization of a rational ruled surface using the $\mu$-basis., Computer Aided Geometric Design, 20 (2003), 11–17.

[CW03a] Chen, F., Wang, W., 2003. The $\mu$-basis of a planar rational curve - properties and computation. Graphical Models 64, 368–381.

[CW03b] Chen, F., Wang, W., 2003. Revisiting the $\mu$-basis of a rational ruled surface. J. Symbolic Comput. 36 (5), 699–716.

[CZS01] Chen, F., Zheng, J., Sederberg, T. W., 2001. The mu-basis of a rational ruled surface. Comput. Aided Geom. Design 18 (1), 61–72.

[Co01] D. A. Cox. Equations of parametric curves and surfaces via syzygies. In *Symbolic computation: solving equations in algebra, geometry, and engineering (South Hadley, MA, 2000)*, volume 286 of *Contemp. Math.*, pages 1–20. Amer. Math. Soc., Providence, RI, 2001.

[Co03a] D. Cox. Curves, surfaces, and syzygies. In *Topics in algebraic geometry and geometric modeling*, volume 334 of *Contemp. Math.*, pages 131–150. Amer. Math. Soc., Providence, RI, 2003.

[Co03b] Cox, David. What is a toric variety?, Topics in algebraic geometry and geometric modeling, Contemp. Math. 334, pp. 203–223, Amer. Math. Soc., Providence, RI. 2003.

[CSC98] Cox, D. A., Sederberg, T. W., Chen, F., 1998. The moving line ideal basis of planar rational curves. Comput. Aided Geom. Design 15 (8), 803–827.

[De02] W.Degen, Cyclides, in Handbook of Computer Aided Geometric Design, 2002, p.575–601

[Do06] M. Dohm, Implicitization of rational ruled surfaces with $\mu$-bases, accepted for publication in Journal of Symbolic Computation, Special Issue EACA 2006, preprint available at http://arxiv.org/pdf/math/0702658

[DZ08] M. Dohm, S. Zube, 2008. The implicit equation of a canal surface. Accepted for publication in Journal of Symbolic Computation.

[Ei95] Eisenbud, D., 1995. Commutative algebra with a view toward algebraic geometry. Vol. 150 of Graduate Texts in Mathematics. Springer-Verlag, New York.

[FGN05] Fioravanti, M., Gonzalez-Vega, L., Necula, I., 2005. Computing the intersection of two ruled surfaces. In: Proc. of Algorithmic Algebra and Logic. Conference in Honor of the 60 th. Birthday of Volker Weispfenning. pp. 187–194.

[Fu84] W. Fulton. *Intersection theory*, volume 2 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1984.

[GKZ94] Gelfand, I.M. and Kapranov, M.M. and Zelevinsky, A.V., Discriminants, resultants, and multidimensional determinants, Birkhäuser Boston Inc., Boston, MA, 1994.

[M2] D. R. Grayson and M. E. Stillman. Macaulay 2, a software system for research in algebraic geometry. Available at http://www.math.uiuc.edu/Macaulay2/.

[HSV83] J. Herzog, A. Simis, and W. V. Vasconcelos. Koszul homology and blowing-up rings. In *Commutative algebra (Trento, 1981)*, volume 84 of *Lecture Notes in Pure and Appl. Math.*, pages 79–169. Dekker, New York, 1983.

[Jo91] Jouanolou, J.-P., 1991. Le formalisme du résultant. Adv. Math. 90, 117–263.

[Ka05] M.Kazakeviciute "Blending of natural quadrics with rational canal surfaces", PhD thesis, Vilnius University, 2005.

[Kr07] R. Krasauskas, Minimal rational parametrizations of canal surfaces, Computing, vol.79 (2007), 281-290.

[KM00] R. Krasauskas, C. Mäurer, Studying cyclides using Laguerre geometry, *Computer Aided Geometric Design* **17** (2000) 101–126.

[KZ07] R. Krasauskas, S. Zube, Canal Surfaces Defined by Quadratic Families of Spheres, in: Geometric Modeling and Algebraic Geometry, B. Jttler, R. Piene (Eds.), Springer, 2007, pp. 138-150. (Publication: November, 2007)

[Kh03] Khetan, A., 2003. The resultant of an unmixed bivariate system. J. Symbolic Comput. 36 (3-4), 425–442, international Symposium on Symbolic and Algebraic Computation (ISSAC'2002) (Lille).

[KD06] A. Khetan and C. D'Andrea. Implicitization of rational surfaces using toric varieties. *J. Algebra*, 303(2):543–565, 2006.

[LSW01] G. Landsmann, J. Schicho and F. Winkler, The parametrization of canal surfaces and the decomposition of polynomials into a sum of two squares, *J. Symbolic Computation* **32** (2001) 119–132.

[LG06] Li, Jia and Gao, Xiaoshan, The proper parametrization of a special class of rational parametric equations, J. Syst. Sci. Complex., 19, 2006, pp. 331–339.

[Ma94] Manocha, D., Solving systems of polynomial equations, Computer Graphics and Applications 14, IEEE, 1994, pp. 46-55.

[MS05] Miller, Ezra and Sturmfels, Bernd. *Combinatorial commutative algebra*, volume 227 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005.

[Pe06] Pérez-Díaz, S., 2006. On the problem of proper reparametrization for rational curves and surfaces. Comput. Aided Geom. Design 23 (4), 307–323.

[PS06] Pérez-Díaz, S. and Sendra, J.R., 2004. Computation of the degree of rational surface parametrizations. J. Pure Appl. Algebra 193, 99–121.

[PP97] M. Peternell and H. Pottmann, Computing rational parametrizations of canal surfaces, *J. Symbolic Computation* **23** (1997) 255–266.

[PP98] H. Pottmann and M. Peternell, Application of Laguerre geometry in CAGD, *Computer Aided Geometric Design* **15** (1998) 165–186.

[PPR98] H. Pottmann, M. Peternell, B. Ravani, Contributions to computational line geometry, *in Geometric Modeling and Procesing '98* (1998) 43–81.

[Pr90] M. J. Pratt, Cyclides in computer aided geometric design, *Computer Aided Geometric Design* **7** (1990) 221–242.

[Pr95] M. J. Pratt, Cyclides in computer aided geometric design II, *Computer Aided Geometric Design* **12** (1995) 131–152.

[SS05] F. San Segundo, J. R. Sendra, Degree Formulae for Offset Curves, Journal of Pure and Applied Algebra, vol 195/3, (2005) 301-335.

[Sc03] Schicho, Josef, Simplification of surface parametrizations—a lattice polygon approach, J. Symbolic Comput. 36, 2003, 3-4, 535–554

[SC95] T. Sederberg and F. Chen. Implicitization using moving curves and surfaces. Computer Graphics Annual Conference Series, pages 301–308, 1995.

[SGD97] Sederberg, T., Goldman, R., and Du, H., Implicitizing rational curves by the method of moving algebraic curves, J. Symbolic Comput. 23, 1997, pp. 153–175.

[SSQK94] Sederberg, T.W., Saito, T., Qi, D.X., and Klimaszewski, K.S., Curve implicitization using moving lines, Comput. Aided Geom. Design 11, 1994, pp. 687–706.

[Sh77] Shafarevich, I. R., 1977. Basic algebraic geometry, study Edition. Springer-Verlag, Berlin, translated from the Russian by K. A. Hirsch, Revised printing of Grundlehren der mathematischen Wissenschaften, Vol. 213, 1974.

[Su06] S. Sullivant, Combinatorial Symbolic Powers, preprint available at http://arxiv.org/abs/math/0608542v3, 2006.

[vdW70] van der Waerden, B. L., 1970. Algebra. Vol 1. Translated by Fred Blum and John R. Schulenberger. Frederick Ungar Publishing Co., New York.

[Va94] W. V. Vasconcelos. *Arithmetic of blowup algebras*, volume 195 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1994.

[XFS06] Z. Xu, R. Feng and J. Sun, Analytic and algebraic properties of canal surfaces, Journal of Computational and Applied Mathematics, 195(1-2), (2006) 220-228.

[Zi91] Zippel, R., 1991. Rational function decomposition. In: Proceedings of the 1991 international symposium on symbolic and algebraic computation. Bonn, Germany, pp. 1–6.

## Implicitisation de surfaces algébriques rationnelles avec la méthode des syzygies

L'implicitisation d'une surface algébrique rationnelle, c'est-à-dire le passage de la paramétrisation à une représentation implicite, est un problème géométrique classique. Dans ce travail de thèse, nous utilisons la théorie des syzygies pour représenter implicitement une surface par une matrice dont les mineurs de taille maximale ont l'équation implicite comme plus grand diviseur commun.

Dans les deux premiers chapitres, nous traitons deux classes de surfaces spéciales pour lesquelles il est toujours possible de construire une matrice carrée qui correspond au résultant d'une $\mu$-base : les surfaces réglées et les surfaces canales. Dans les chapitres suivants, le cas général de surfaces rationnelles paramétrées sur une variété torique de dimension 2 est étudié. Nous montrons qu'une telle matrice peut être construite en n'utilisant que des syzygies linéaires et nous décrivons un algorithme simple et efficace pour son calcul.

**Mots clés :** implicitisation, syzygy, représentation matricielle, complèxe d'approximation, géométrie algébrique, algèbre commutative, C.A.O.

## Implicitization of rational algebraic surfaces with syzygy-based methods

The implicitization of a rational algebraic surface, i.e. the passage from a parametrization to an implicit representation, is a classical geometric problem. In this thesis we use the theory of syzygies to represent a surface implicitly by a matrix whose maximal-sized minors have the implicit equation of the surface as their greatest common divisor.

In the first two chapters, we treat two special classes of surfaces for which it is always possible to construct a square representation matrix corresponding to the resultant of a $\mu$-basis: ruled surfaces and canal surfaces. In the following chapters, the general case of rational surfaces parametrized over a two-dimensional toric variety is studied. We show that a representation matrix can be constructed only using linear syzygies and we give a simple and efficient algorithm for its computation.

**Keywords :** implicitization, syzygy, matrix representation, approximation complex, algebraic geometry, commutative algebra, CAGD