MONOGRAFÍAS
DE LA
REAL ACADEMIA
DE CIENCIAS
Exactas
Físicas
Químicas y
Naturales
DE
ZARAGOZA

Nº 43

Proceedings of the XVI EACA Zaragoza

Encuentros de Álgebra Computacional y Aplicaciones

E. Artal y J.I. Cogolludo (Editores)

2018

ISSN: 1132-6360

ÍNDICE DE MATERIAS

Preface

EACA stands for "Encuentros de Álgebra Computacional y Aplicaciones" (Meetings on Computer Algebra and Applications). These meetings are organized by the Spanish "Red Temática de Cálculo Simbólico, Álgebra Computacional y Aplicaciones" (EACA Network on Symbolic Computation, Computer Algebra and Applications). Their purpose is two-fold: first to provide an appropriate meeting point both for researchers specialized in developing these areas and for those who use them in their own research activities, and second to support and encourage participation by young researchers.

These meetings started in Santander in 1995 and have been held annually in Sevilla, Granada, Sigüenza, Tenerife, Barcelona, and Ezcaray. Starting in 2002 in Valladolid they have been held biannually in Santander, Sevilla, Granada, Santiago de Compostela, Alcalá de Henares, Barcelona, and most recently in Logroño in 2016. The 16th edition is being held in Zaragoza in July, 2018.

The EACA Network organizes a variety of International Schools, workshops, and symposia focusing on the following subject areas:

- Effective Methods in Algebra, Analysis, Geometry and Topology,
- Algorithmic Complexity,
- Scientific Computation by means of Symbolic-Numerical Methods,
- Symbolic-Numeric Software Development,
- Analysis, Specification, Design and Implementation of Symbolic Computation Systems,
- Applications in Science and Technology.

It is noteworthy to point out that over the years these meetings have achieved greater international recognition, especially from members of the Symbolic Computation community. Proof of that is the increasing number of high-standard publications citing presentations or notes from mini-courses given at EACA. A good example of this is Springer's Lecture Notes in Mathematics 2176 *Computations and Combinatorics in Commutative Algebra* edited by Anna M. Bigatti, Philippe Gimenez, and Eduardo Sáenz-de-Cabezón which stems from the 4th EACA International School in Valladolid in 2013.

EACA 2018 will take place in Zaragoza, at the School of Science of the University of Zaragoza, July 4-6, 2018, preceded by the Sage Days 94 event for developers. Sage Days offer developers the opportunity to meet and share their latest work on this meeting's background theme: Symbolic Computation. This 94th edition is especially oriented to

young researchers that want to make the transition from writing code for their own use, to contributing to the `Sagemath` codebase.

This book contains the extended abstracts of the accepted contributions and the plenary talks for this 16th edition of EACA. There is a total of 28 contributions, accepted after a standard referee process, and 5 plenary talks. The plenary speakers are:

- Javier Arsuaga, University of California at Davis (USA),
- Anne Frühbis-Krüger, Leibniz Universität Hannover (Germany),
- Javier Lobillo, Universidad de Granada (Spain),
- Fatemeh Mohammadi, University of Bristol (UK), and
- Ana Romero, Universidad de La Rioja (Spain).

We would like to express our sincere gratitude to all the organizers, especially to the members of the Scientific Committee chaired by Francisco J. Castro (U. de Sevilla): María Emilia Alonso (U. Complutense de Madrid), Isabel Bermejo (U. de La Laguna), Marta Casanellas (U. Politècnica de Catalunya), Carlos D'Andrea (U. de Barcelona), Philippe Gimenez (U. de Valladolid), José Gómez-Torrecillas (U. de Granada), Laureano González-Vega (U. de Cantabria), Manuel Ladra (U. de Santiago de Compostela), Sonia Pérez (U. de Alcalá), and Ana Romero (U. de la Rioja). Our gratitude also goes to the University of Zaragoza, the IUMA (UZ Math and Applications Insitute), and the local committee: Enrique Artal, José Ignacio Cogolludo, Jorge Martín, Miguel Marco, Rubén Blasco, and Juan Serrano for making this event possible. Special thanks should be given to all the institutions that have offered us financial support such as:

- Universidad de Zaragoza,
- Instituto Universitario de Matemáticas y sus Aplicaciones
- Departamento de Matemáticas,
- Ministerio de Economía y Competitividad,

Last, but not least, these meetings strengthen the personal and professional links in the Network; they are a great opportunity to meet and have discussions on the latest problems and their possible solutions. We hope the university facilities as well as the city of Zaragoza serve as a catalyst towards this purpose and wish all participants a pleasant and productive stay.

E. Artal and J.I. Cogolludo
IUMA, Universidad de Zaragoza

PLENARY TALKS

Monografías de la Real Academia de Ciencias. Zaragoza. **43:** 13–13, (2018).
ISSN: 1132-6360

ALGEBRAIC ANALYSIS OF CANCER GENOMES

JAVIER ARSUAGA

The cancer genome is characterized by large-scale structural changes of chromosomes, called chromosome aberrations. Chromosome aberrations occur as exchanges between different chromosomes (this is the case of the exchange between chromosomes 9 and 22 that characterizes chronic myeloid leukemia) and as changes in the number of copies of any genomic region (as it is the case for the copy number gain of the long arm of chromosome 17 –*i.e.* 17q– in certain breast cancer patients). Identification of these aberrations is important and challenging. It is important because they commonly house cancer-driving genes; it is challenging because of the variability observed across patients. In this talk, I will illustrate how algebraic statistics and algebraic topology can be used to detect chromosome exchanges and copy number changes respectively.

A key step in the formation of exchange type chromosome aberrations is the breakage of chromosomes that are in close spatial proximity. To test for the statistical significance of spatial proximity of chromosomes, we build log-linear models and perform maximum likelihood estimation on tables whose entries are given by the frequency of chromosome exchanges. When the entries in these tables are large, traditional statistical methods can be used. However, since small entries are present, algebraic methods are called for. In particular, we use Markov bases to generate null distributions of tables. We tested this method on a set of tables of radiation induced chromosome aberrations on human lymphocyte and found significance of chromosomes $\{1, 22\}$ and $\{13, 14\}$. Both pairs of chromosomes had been previously reported to be in close proximity.

To identify chromosome copy number changes in a population of patients, we use methods from persistence homology that associate a set of Vietoris-Rips simplicial complexes to each patient profile. We use the rank of the zero homology group (β_0) of the complexes to detect localized copy number changes, and the rank of the zero homology group (β_1) to analyze the finer structure of the aberrations that spread over entire chromosome arms. We applied this method to identify copy number changes specific to the four different breast cancer molecular subtypes (Luminal A, Luminal B, Basal-like and ERBB2 amplified). When using β_0, we obtained many of the aberrations previously reported, and identified three new aberrations in the basal-like subtype: 1p, 2p and 14q. Using β_1, we identified three regions within the arm 17q that are simultaneously gained in multiple ERBB2 amplified patients ($17q12$, $17q21.2$ and $17q21.33$). This frequent presence of these aberrations suggests a role in tumor development.

Department of Molecular and Cellular Biology Department of Mathematics, University of California Davis, Davis USA

E-mail address: jarsuaga@ucdavis.edu

Monografías de la Real Academia de Ciencias. Zaragoza. **43:** 15–15, (2018).
ISSN: 1132-6360

MASSIVELY PARALLEL COMPUTATIONS AND ALGEBRAIC GEOMETRY – A CONTRADICTION?

ANNE FRÜHBIS-KRÜGER

While massively parallel computations are ubiquitous in numerics and simulation, they have rarely ever been thought about in computational algebraic geometry – and for good reasons, many would say. Already the Gröbner Basis Algorithm, which is the workhorse behind numerous computations, does not have a natural parallelization and thus seems to be a huge obstacle. But there are tasks in algebraic geometry, which are accessible to a very coarse grained, massively parallel approach due to the local nature of the problem itself. In this talk, I will show a few examples, in which such an approach proved fruitful such as e.g. a smoothness test based on the termination criterion of Hironaka's resolution of singularities.

Institut für Algebraische Geometrie, Leibniz Universität Hannover,
Welfengarten 1, 30167 Hannover, Germany

e-mail address: anne@math.uni-hannover.de

Monografías de la Real Academia de Ciencias. Zaragoza. **43:** 17–17, (2018).
ISSN: 1132-6360

SKEW POLYNOMIALS, ERROR CORRECTING CODES AND MCELIECE CRYPTOSYSTEM

F.J. LOBILLO

Abstract. In the last years, skew polynomials have been used in the design of error correcting codes with good distances and their corresponding fast algebraic decoding algorithms. Concretely, the σ-codes use similarity of the arithmetic of polynomials and skew polynomials to study σ-cyclic structures on block and concolutional codes. Non commutative key equations have also been derived, which opens the door to design Sugiyama's like decoding algorithms. The Peterson-Gorenstein-Zierler approach to decode cyclic codes can be adapted to the skew cyclic framework too. The correspondence of skew and linearized polynomials allows to connect σ-cyclic codes with Gabidulin codes and the rank metric. Since these families of codes can be efficiently decoded, they are candidates to replace Goppa codes in the McEliene cryptosystem. We will explore current succesful attacks to some of them.

CITIC and Department of Algebra, University of Granada, Spain

e-mail address: jlobillo@ugr.es

Monografías de la Real Academia de Ciencias. Zaragoza. **43:** 19–19, (2018).
ISSN: 1132-6360

COMPUTING TORIC DEGENERATIONS OF GRASSMANNIANS AND FLAG VARIETIES ARISING FROM TROPICAL GEOMETRY

FATEMEH MOHAMMADI

Abstract. A toric variety is a certain algebraic variety modeled on a convex polyhedron. Toric varieties play an important role in commutative algebra. I give an overview talk on toric degenerations of flag varieties and Grassmannians arising from tropical geometry and representation theory. I will compare toric degenerations arising from string polytopes with those obtained from tropical cones of flag varieties and will explain how the corresponding toric polytopes can be seen as Newton-Okounkov bodies for the valuations associated to each tropical cone. I will also present the necessary condition to obtain a toric initial ideal of Grassmannian of 3-planes explaining computational challenges around this problem. This is based on joint works with Kristin Shaw and with Lara Bossinger, Sara Lamboglia, and Kalina Mincheva.

School of Mathematics, University of Bristol, Bristol, BS8 1TW, UK

e-mail address: fatemeh.mohammadi@bristol.ac.uk

Monografías de la Real Academia de Ciencias. Zaragoza. **43:** 21–24, (2018).
ISSN: 1132-6360

A COMPUTATIONAL REVIEW OF SPECTRAL SEQUENCES AND APPLICATIONS

ANA ROMERO

Abstract. In this work we present some algorithms and programs for computing different types of spectral sequences, a useful tool of Algebraic Topology which has been frequently used in order to compute homology and homotopy groups of spaces. The programs make it possible to determine all components of spectral sequences even when the initial spaces are not of finite type. Moreover, the programs have been applied in other contexts to determine persistent homology, homology of groups, spectral systems and homology of finite topological spaces.

Introduction

Spectral sequences are a useful technique in Algebraic Topology traditionally applied to calculate homology and homotopy groups of spaces (see [Mac63] or [McC85]). The Serre spectral sequence [Ser51], for example, gives information about the homology groups of the total space of a fibration when the homology groups of the base and fiber spaces are known. On the other hand, the Eilenberg-Moore spectral sequences [EM65] give information about the homology groups of the base space (resp. the fiber space) from the homologies of the total space and of the fiber (resp. base space). For the computation of homotopy groups, the spectral sequences of Adams [Ada60] or Bousfield-Kan [BK72] can be used. And many other examples of spectral sequences can be found in the literature: Bockstein, Grothendieck, Hurewicz, Künneth, Quillen, Van Kanpen, etc.

A spectral sequence is a family of "pages" $(E^r_{p,q}, d^r)_{r\geq 1}$ of differential bigraded modules as in Figure 1, each page being made of the homology groups of the preceding one. In many situations, a formula is given only for the first page of the spectral sequence, but then the following levels can only be determined when the initial space is of finite type (a situation which is not very frequent) or in particular cases where many of the groups $E^r_{p,q}$'s of the first level are zero.

In this work, we present a set of algorithms and programs for computing spectral sequences implemented in the system Kenzo [DRSS99], a program devoted to Symbolic Computation in Algebraic Topology, which has made it possible to determine homology and homotopy groups of complicated spaces of infinite type. The programs can be applied for computing the classical examples of spectral sequences of Serre and Eilenberg-Moore (also for infinite type spaces) and in other different situations such as the computation of persistent homology, homology of groups, spectral systems and homology of finite topological spaces.

Partially supported by Ministerio de Economía, Industria y Competitividad, Spain, project MTM2017-88804-P.

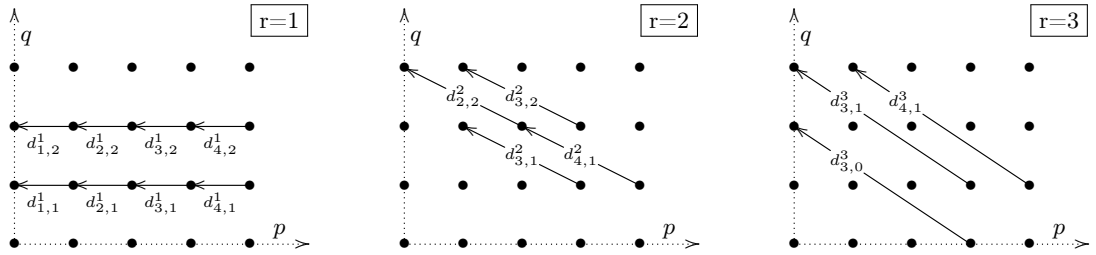


FIGURE 1. First levels of a first quadrant spectral sequence.

1. Spectral sequences of filtered complexes

In [RRS06], a set of algorithms and programs was developed for computing spectral sequences of filtered complexes, a particular type of spectral sequence defined in terms of a filtration $\ldots \subseteq F_{p-1}C_* \subseteq F_pC_* \subseteq F_{p+1}C_* \subseteq \ldots$ of a chain complex C_*. The spectral sequence produces then a sequence of groups which, in a suitable sense, "converges" to the homology groups of C_*. Although in this case a formal expression for the different groups $E^r_{p,q}$'s (as quotients of some subgroups of the filtered complex C_*) is known [McC85] for all levels of the spectral sequence, this expression can only be directly determined when the initial filtered complex is of finite type.

Our programs were implemented in the Kenzo system by using the technique of *effective homology* (see [RS02]). The programs work in a similar way to the method that Kenzo uses to determine homology groups of a given chain complex: if a filtered complex C_* is of finite type, its spectral sequence can be determined by means of diagonalization algorithms on some matrices. Otherwise, a pair of *reductions* $C_* \nleftarrow\!\!\!\Leftarrow \hat{C}_* \Rightarrow\!\!\!\!\!\!\Rightarrow D_*$ from the initial chain complex C_* to another one D_* of finite type (also filtered) is constructed. The chain complex D_* is called *effective*. In this way, it is possible to determine all components of the spectral sequence even when the filtered chain complex is not of finite type. In particular, these programs can be applied to determine the classical spectral sequences of Serre and Eilenberg-Moore.

2. Bousfield-Kan spectral sequence

The Bousfield-Kan spectral sequence was introduced in [BK72] to establish the Adams spectral sequence [Ada60] on a simplicial combinatorial background. Under some good conditions, the Bousfield-Kan spectral sequence associated with a simplicial set X converges to the homotopy groups of X, $\pi_*(X)$. This spectral sequence is not defined by means of a filtered complex and more complicated structures such as towers of fibrations and cosimplicial spaces are involved in the construction (see [BK72] for details).

In [RS17], an algorithm was developed computing the Bousfield-Kan spectral sequence associated with a simplicial set X which has effective homology. This algorithm is not related with the one presented in Section 1 and requires the use of a new theory, called *effective homotopy*, inspired by the technique of effective homology and introduced in [RS12]. The main ingredient of the algorithm computing this spectral sequence consists in constructing the effective homotopy of the different elements in the tower of fibrations which appears in the definition of the spectral sequence. The algorithm can be applied to 1-reduced simplicial

sets X with effective homology, allowing in particular the computation of stable and unstable homotopy groups of spheres. Moreover, we are able to compute the natural filtration induced on the homotopy groups by the spectral sequence.

3. Applications

Our algorithms and programs computing spectral sequences have also been used in other contexts and applications.

First of all, in [RHRS14] we shown the existing relation between spectral sequences and persistent homology for integer coefficients. Then, a slight modification of our programs computing spectral sequences of filtered complexes presented in Section 1 made it possible to compute also persistent homology. By inheritance from our spectral sequence programs, we obtained for free persistent homology programs applicable to spaces not of finite type (provided they are spaces with effective homology) and with $\mathbb{Z}$-coefficients (significantly generalizing the usual presentation of persistent homology over a field).

On the other hand, the notion of spectral sequence has been recently generalized by Benjamin Matschke in [Mat13] to filtrations of chain complexes indexed over any partially ordered set, rather than being limited to filtrations indexed over the set $\mathbb{Z}$ of integer numbers as for classical spectral sequences. The collection of groups produced by his generalized construction is called *spectral system* and is related with multipersistence. Thanks again to the effective homology method and using also the technique of Discrete Vector Fields [RS10], a set of programs has been developed in [GR18] computing generalized spectral sequences.

Finally, in a recent and ongoing work, our programs for computing spectral sequences have also been applied for the computation of homology of groups and homology of finite topological spaces.

References

[Ada60] J. F. Adams. On the non-existence of elements of Hopf invariant one. *Annals of Mathematics*, 72(1):20–104, 1960.

[BK72] A.K. Bousfield and D.M. Kan. *Homotopy Limits, Completions and Localizations*. Lecture Notes in Mathematics vol. 304. Springer-Verlag, 1972.

[DRSS99] X. Dousson, J. Rubio, F. Sergeraert, and Y. Siret. The Kenzo program. `http://www-fourier.ujf-grenoble.fr/~sergerar/Kenzo/`, 1999.

[EM65] S. Eilenberg and J. C. Moore. Homology and fibrations, I: Coalgebras, cotensor product and its derived functors. *Commentarii Mathematici Helvetici*, 40:199–236, 1965.

[GR18] A. Guidolin and A. Romero. Effective computation of generalized spectral sequences. To appear in Proceedings of International Symposium on Symbolic and Algebraic Computation, 2018.

[Mac63] S. MacLane. *Homology*, volume 114. Springer, 1963.

[Mat13] B. Matschke. Successive spectral sequences. Preprint. `http://arxiv.org/abs/1308.3187v1`, 2013.

[McC85] J. McCleary. *User's guide to spectral sequences*. Publish or Perish, 1985.

[RHRS14] A. Romero, J. Heras, J. Rubio, and F. Sergeraert. Defining and computing persistent $\mathbb{Z}$-homology in the general case. Preprint. `http://arxiv.org/abs/1403.7086`, 2014.

[RRS06] A. Romero, J. Rubio, and F. Sergeraert. Computing spectral sequences. *Journal of Symbolic Computation*, 41(10):1059–1079, 2006.

[RS02] J. Rubio and F. Sergeraert. Constructive Algebraic Topology. *Bulletin des Sciences Mathématiques*, 126(5):389–412, 2002.

[RS10] A. Romero and F. Sergeraert. Discrete Vector Fields and fundamental Algebraic Topology. Preprint. `http://arxiv.org/abs/1005.5685v1`, 2010.

[RS12] A. Romero and F. Sergeraert. Effective homotopy of fibrations. *Applicable Algebra in Engineering, Communication and Computing*, 23:85–100, 2012.

[RS17] A. Romero and F. Sergeraert. A Bousfield-Kan algorithm for computing the effective homotopy of a space. *Foundations of Computational Mathematics*, 17(5):1335–1366, 2017.

[Ser51] J. P. Serre. Homologie singulière des espaces fibrés. *Annals of Mathematics*, 54(3):425–505, 1951.

Universidad de La Rioja. c/Madre de Dios 53. 26006 Logroño, Spain.
E-mail address: ana.romero@unirioja.es

CONTRIBUTED TALKS

Monografías de la Real Academia de Ciencias. Zaragoza. **43:** 27–30, (2018).
ISSN: 1132-6360

POINCARÉ SERIES FOR MIXED MULTIPLIER IDEALS

MARIA ALBERICH-CARRAMIÑANA, JOSEP ÀLVAREZ MONTANER, FERRAN DACHS-CADEFAU, AND VÍCTOR GONZÁLEZ-ALONSO

Abstract. We present a generalization of the Poincaré series to the case of mixed multiplier ideals. For that, we will recall some results about how we can compute the jumping walls associated to a mixed multiplier ideal and introduce some results about the multiplicity of a given point in $\mathbb{R}^r_{\geqslant 0}$.

Introduction

Let X be a complex surface with at most a rational singularity at a point $O \in X$ (see Artin [3] and Lipman [8] for details) and $\mathfrak{m} = \mathfrak{m}_{X,O}$ be the maximal ideal of the local ring $\mathcal{O}_{X,O}$ at O. Given a tuple of $\mathfrak{m}$-primary ideals $\mathfrak{a} := \{\mathfrak{a}_1, ..., \mathfrak{a}_r\} \subseteq (\mathcal{O}_{X,O})^r$ we will consider a common *log-resolution*, that is a birational morphism $\pi : X' \to X$ such that X' is smooth, $\mathfrak{a}_i \cdot \mathcal{O}_{X'} = \mathcal{O}_{X'}(-F_i)$ for some effective Cartier divisors F_i, $i = 1, \ldots, r$ and $\sum_{i=1}^r F_i + E$ is a divisor with simple normal crossings where $E = Exc(\pi)$ is the exceptional locus. Actually, the divisors F_i are supported on the exceptional locus since the ideals are $\mathfrak{m}$-primary.

Since the point O has (at worst) a rational singularity, the exceptional locus E is a tree of smooth rational curves $E_1, \ldots, E_s$. Moreover, the matrix of intersections $(E_i \cdot E_j)_{1 \leqslant i,j \leqslant s}$ is negative-definite. For any exceptional component E_j, we define the *excess* of $\mathfrak{a}_i$ at E_j as $\rho_{i,j} = -F_i \cdot E_j$. We also recall the following notions:

- A component E_j of E is a *rupture* component if it intersects at least three more components of E (different from E_j).
- We say that E_j is *dicritical* if $\rho_{i,j} > 0$ for some i. They correspond to *Rees valuations* (see [8]).

We define the *mixed multiplier ideal* at a point $\mathbf{c} := (c_1, .., c_r) \in \mathbb{R}^r_{\geqslant 0}$ as [1]

$$\mathcal{J}(\mathfrak{a}^{\mathbf{c}}) := \mathcal{J}(\mathfrak{a}_1^{c_1} \cdots \mathfrak{a}_r^{c_r}) = \pi_* \mathcal{O}_{X'}(\lceil K_\pi - c_1 F_1 - \cdots - c_r F_r \rceil) \tag{1}$$

where $\lceil \cdot \rceil$ denotes the *round-up* and the *relative canonical divisor* $K_\pi = \sum_{i=1}^s k_j E_j$ is a $\mathbb{Q}$-divisor on X' supported on the exceptional locus E which is characterized by the property $(K_\pi + E_i) \cdot E_i = -2$ for every exceptional component E_i, $i = 1, \ldots, s$.

Associated to any point $\boldsymbol{c} \in \mathbb{R}^r_{\geqslant 0}$, we consider:

All four authors are partially supported by Spanish Ministerio de Economía y Competitividad MTM2015-69135-P. MAC and JAM are also supported by Generalitat de Catalunya SGR2017-932 project and they are with the Barcelona Graduate School of Mathematics (BGSMath). MAC is also with the Institut de Robòtica i Informàtica Industrial (CSIC-UPC).

[1] By an abuse of notation, we will also denote $\mathcal{J}(\mathfrak{a}^{\mathbf{c}})$ its stalk at O so we will omit the word "sheaf" if no confusion arises.

- The *region* of $\boldsymbol{c}$: $\mathcal{R}_{\mathfrak{a}}(\boldsymbol{c}) = \left\{\boldsymbol{c}' \in \mathbb{R}^r_{\geqslant 0} \;\middle|\; \mathcal{J}\left(\mathfrak{a}^{\boldsymbol{c}'}\right) \supseteq \mathcal{J}\left(\mathfrak{a}^{\boldsymbol{c}}\right)\right\}$
- The *constancy region* of $\boldsymbol{c}$: $\mathcal{C}_{\mathfrak{a}}(\boldsymbol{c}) = \left\{\boldsymbol{c}' \in \mathbb{R}^r_{\geqslant 0} \;\middle|\; \mathcal{J}\left(\mathfrak{a}^{\boldsymbol{c}'}\right) = \mathcal{J}\left(\mathfrak{a}^{\boldsymbol{c}}\right)\right\}$

The boundary of the region $\mathcal{R}_{\mathfrak{a}}(\boldsymbol{c})$ is what we call the *jumping wall* associated to $\boldsymbol{c}$. One usually refers to the jumping wall of the origin as the *log-canonical wall*. It follows from the definition of mixed multiplier ideals that the jumping walls must lie on *supporting hyperplanes* of the form

$$H_j : \; e_{1,j}z_1 + \cdots + e_{r,j}z_r = \ell + k_j \qquad j = 1, \ldots, s \tag{2}$$

where $\ell \in \mathbb{Z}_{>0}$, and the effective divisors F_i such that $\mathfrak{a}_i \cdot \mathcal{O}_{X'} = \mathcal{O}_{X'}(-F_i)$, for $i = 1, \ldots, r$, are of the form $F_i = \sum_{j=1}^{s} e_{i,j}E_j$. Indeed, each hyperplane H_j is associated to an exceptional divisor E_j and the region $\mathcal{R}_{\mathfrak{a}}(\boldsymbol{c})$ is a *rational convex polytope* defined by

$$e_{1,j}z_1 + \cdots + e_{r,j}z_r < \ell + k_j,$$

i.e. the minimal region in the positive orthant $\mathbb{R}^r_{\geqslant 0}$ described by these inequalities. Notice that the facets of the jumping wall of $\boldsymbol{c}$ are also rational convex polytopes. From now on we will denote by $\mathbf{JW}_{\mathfrak{a}}$ the set of jumping walls of $\mathfrak{a}$.

One can characterize which hyperplanes define the region of a given point $\boldsymbol{\lambda}$, namely:

Theorem 0.1 (see Theorem 3.3 in [2])**.** *Let $\mathfrak{a} := \{\mathfrak{a}_1, ..., \mathfrak{a}_r\} \subseteq (\mathcal{O}_{X,O})^r$ be a tuple of ideals and let $D_{\boldsymbol{\lambda}} = \sum e_j^{\boldsymbol{\lambda}} E_j$ be the antinef closure of $\lfloor \lambda_1 F_1 + \cdots + \lambda_r F_r - K_\pi \rfloor$ for a given $\boldsymbol{\lambda} \in \mathbb{R}^r_{\geqslant 0}$. Then the region of $\boldsymbol{\lambda}$ is the rational convex polytope determined by the inequalities*

$$e_{1,j}z_1 + \cdots + e_{r,j}z_r < k_j + 1 + e_j^{\boldsymbol{\lambda}},$$

corresponding to either rupture or dicritical divisors E_j.

1. An algorithm to compute mixed multiplier ideals and jumping walls

In [2], the first three authors presented the following algorithm. This algorithm allows us to compute for a given tuple of ideals the associated jumping walls.

Algorithm 1.1 (see Algorithm 3.11 in [2])**.** (Constancy regions and mixed multiplier ideals)

`Input:` A common log-resolution of the tuple of ideals $\mathfrak{a} = \{\mathfrak{a}_1, \ldots, \mathfrak{a}_r\} \subseteq (\mathcal{O}_{X,O})^r$.
`Output:` List of constancy regions of $\mathfrak{a}$ and its corresponding mixed multiplier ideals.

Set $N = \{\boldsymbol{\lambda}_0 = (0, \ldots, 0)\}$ and $D = \emptyset$. From $j = 1$, incrementing by 1

(Step j) :

(j.1) **Choosing a convenient point in the set** N:
- Pick $\boldsymbol{\lambda}_j$ the first point in the set N and compute its region $\mathcal{R}_{\mathfrak{a}}(\boldsymbol{\lambda}_j)$ using Theorem 0.1.
- If there is some $\boldsymbol{\lambda} \in N$ such that $\boldsymbol{\lambda} \in \mathcal{R}_{\mathfrak{a}}(\boldsymbol{\lambda}_j)$ and $\mathcal{J}(\mathfrak{a}^{\boldsymbol{\lambda}}) \neq \mathcal{J}(\mathfrak{a}^{\boldsymbol{\lambda}_j})$ then put $\boldsymbol{\lambda}$ first in the list N and repeat this step (j.1). Otherwise continue with step (j.2).

(j.2) **Checking out whether the region has been already computed**:
- If some $\boldsymbol{\lambda} \in D$ satisfies $\mathcal{J}(\mathfrak{a}^{\boldsymbol{\lambda}}) = \mathcal{J}(\mathfrak{a}^{\boldsymbol{\lambda}_j})$ then go to step (j.4). Otherwise continue with step (j.3).

(j.3) **Picking new points for which we have to compute its region**:
- Compute
$$\mathcal{C}(j) = \mathcal{R}_{\mathfrak{a}}(\boldsymbol{\lambda}_j) \setminus (\mathcal{R}_{\mathfrak{a}}(\boldsymbol{\lambda}_1) \cup \cdots \cup \mathcal{R}_{\mathfrak{a}}(\boldsymbol{\lambda}_{j-1}))\,.$$
- For each connected component of $\mathcal{C}(j)$ compute its outer facets[2].
- Pick one interior point in each outer facet of $\mathcal{C}(j)$ and add them as the last point in N.

(j.4) **Update the sets N and D**:
- Delete $\boldsymbol{\lambda}_j$ from N and add $\boldsymbol{\lambda}_j$ as the last point in D.

2. Multiplicities of jumping points

The goal of this section is to study the Poincaré series associated to a mixed multiplier ideal. For that, we need to begin introducing the notion of multiplicity. Namely, if we consider $\mathfrak{a} = (\mathfrak{a}_1, \ldots, \mathfrak{a}_r) \subseteq (\mathcal{O}_{X,O})^r$ a tuple of $\mathfrak{m}$-primary ideals. We define the multiplicity attached to a point $\boldsymbol{c} \in \mathbb{R}^r_{\geqslant 0}$ as the codimension of $\mathcal{J}(\mathfrak{a}^{\boldsymbol{c}})$ in $\mathcal{J}\left(\mathfrak{a}^{(1-\varepsilon)\boldsymbol{c}}\right)$ for $\varepsilon > 0$ small enough, i.e.

$$m(\boldsymbol{c}) := \dim_{\mathbb{C}} \frac{\mathcal{J}\left(\mathfrak{a}^{(1-\varepsilon)\boldsymbol{c}}\right)}{\mathcal{J}\left(\mathfrak{a}^{\boldsymbol{c}}\right)}\,.$$

Our goal is to compute explicitly these multiplicities. Since we are dealing with any general point, it will be convenient to consider the notion of *maximal jumping divisor*.

Definition 2.1. Let $\mathfrak{a} := (\mathfrak{a}_1, \ldots, \mathfrak{a}_r) \subseteq (\mathcal{O}_{X,O})^r$ be a tuple of ideals. Given any point $\boldsymbol{c} \in \mathbb{R}^r_{\geqslant 0}$, we define its *maximal jumping divisor* as the reduced divisor $H_{\boldsymbol{c}} \leqslant \sum_{i=1}^r F_i$ supported on those components E_j such that

$$c_1 e_{1,j} + \cdots + c_r e_{r,j} - k_j \in \mathbb{Z}_{>0}\,.$$

In particular, we have

$$\mathcal{J}(\mathfrak{a}^{(1-\varepsilon)\boldsymbol{c}}) = \pi_* \mathcal{O}_{X'}(\lceil K_\pi - c_1 F_1 - \cdots - c_r F_r \rceil + H_{\boldsymbol{c}})\,,$$

In fact, we can compute the multiplicity using those divisors:

Theorem 2.2. *Let $\mathfrak{a} \subseteq (\mathcal{O}_{X,O})^r$ be a tuple of $\mathfrak{m}$-primary ideals and $H_{\boldsymbol{c}}$ the maximal jumping divisor associated to some $\boldsymbol{c} \in \mathbb{R}^r_{>0}$. Then,*

$$m\left(\boldsymbol{c}\right) = (\lceil K_\pi - c_1 F_1 - \cdots - c_r F_r \rceil + H_{\boldsymbol{c}}) \cdot H_{\boldsymbol{c}} + \#\left\{\textit{connected components of } H_{\boldsymbol{c}}\right\}.$$

2.1. **Poincaré series of mixed multiplier ideals.** Given a $\mathfrak{m}$-primary ideal $\mathfrak{a} \subseteq \mathcal{O}_{X,O}$, Galindo and Montserrat [6] (see also [1]) introduced its *Poincaré series* as

$$P_{\mathfrak{a}}(t) = \sum_{c \in \mathbb{R}_{>0}} m(c)\, t^c. \tag{3}$$

For a tuple of $\mathfrak{m}$-primary ideals $\mathfrak{a} = \{\mathfrak{a}_1, \ldots, \mathfrak{a}_r\} \subseteq (\mathcal{O}_{X,O})^r$ we are going to give a generalization of this series by considering a sequence of mixed multiplier ideals indexed by

[2]The outer facets of $\mathcal{C}(j)$ are the intersection of the boundary of any connected component of $\mathcal{C}(j)$ with a supporting hyperplane of $\mathcal{R}_{\mathfrak{a}}(\boldsymbol{\lambda}_j)$.

points in a ray $L : \boldsymbol{c}_0 + \mu\mathbf{u}$ in the positive orthant $\mathbb{R}^r_{>0}$ with a vector $\mathbf{u} = (u_1, \ldots, u_r) \in \mathbb{Z}^r_{\geqslant 0}$, $\mathbf{u} \neq \mathbf{0}$ and $\boldsymbol{c}_0 \in \mathbb{Q}^r_{\geqslant 0}$. Here we are considering, for simplicity, a point $\boldsymbol{c}_0$ belonging to a coordinate hyperplane but not necessarily being the origin and $\mu \in \mathbb{R}_{>0}$. Namely, we consider the sequence of mixed multiplier ideals

$$\mathcal{J}\left(\mathfrak{a}^{\boldsymbol{c}_0}\right) \supsetneq \mathcal{J}\left(\mathfrak{a}^{\boldsymbol{c}_1}\right) \supsetneq \mathcal{J}\left(\mathfrak{a}^{\boldsymbol{c}_2}\right) \supsetneq \cdots \supsetneq \mathcal{J}\left(\mathfrak{a}^{\boldsymbol{c}_i}\right) \supsetneq \cdots$$

where $\{\boldsymbol{c}_i\}_{i>0} = L \cap \mathbf{JW}_{\mathfrak{a}}$ or equivalently $\{\boldsymbol{c}_i\}_{i>0}$ is the set of jumping points of this sequence. Then we define the *Poincaré series of* $\mathfrak{a}$ *alongside the ray* L as

$$P_{\mathfrak{a}}(\underline{t}; L) = \sum_{\boldsymbol{c} \in L} m(\boldsymbol{c})\, \underline{t}^{\boldsymbol{c}}. \tag{4}$$

where $\underline{t}^{\boldsymbol{c}} := t_1^{c_1} \cdots t_r^{c_r}$.

Theorem 2.3. *Let* $\mathfrak{a} = \{\mathfrak{a}_1, \ldots, \mathfrak{a}_r\} \subseteq (\mathcal{O}_{X,O})^r$ *be a tuple of* $\mathfrak{m}$*-primary ideals and* $L : \boldsymbol{c}_0 + \mu\mathbf{u}$ *a ray in the positive orthant* $\mathbb{R}^r_{>0}$. *The Poincaré series of* $\mathfrak{a}$ *alongside* L *can be expressed as*

$$P_{\mathfrak{a}}(\underline{t}; L) = \underline{t}^{\boldsymbol{c}_0} \sum_{\mu \in [0,1]} \left(\frac{m(\boldsymbol{c}_0 + \mu\mathbf{u})}{1 - \underline{t}^{\mathbf{u}}} + \rho_{\boldsymbol{c},\mathbf{u}} \frac{\underline{t}}{(1 - \underline{t}^{\mathbf{u}})^2} \right) \underline{t}^{\mu\mathbf{u}}\,.$$

References

[1] M. Alberich-Carramiñana, J.Àlvarez Montaner, F. Dachs-Cadefau and V. González-Alonso, *Poincaré series of multiplier ideals in two-dimensional local rings with rational singularities*, Adv. Math. **304** (2017), 769–792.

[2] M. Alberich-Carramiñana, J.Àlvarez Montaner and F. Dachs-Cadefau, *Constancy regions of mixed multiplier ideals in two-dimensional local rings with rational singularities*, Math. Nachr. **291** (2018), 219–517

[3] M. Artin, *On isolated rational singularities of surfaces*, Amer. J. Math. **68** (1966), 129–136.

[4] Pi. Cassou-Noguès and A. Libgober, *Multivariable Hodge theoretical invariants of germs of plane curves*, J. Knot Theory Ramifications **20** (2011), 787–805.

[5] Pi. Cassou-Noguès and A. Libgober, *Multivariable Hodge theoretical invariants of germs of plane curves II*, in Valuation Theory in Interaction. Eds. A Campillo, F.-V. Kuhlmann and B. Teissier. EMS Series of Congress Reports **10** (2014), 82–135.

[6] C. Galindo and F. Monserrat, *The Poincaré series of multiplier ideals of a simple complete ideal in a local ring of a smooth surface*, Adv. Math. **225** (2010), 1046–1068.

[7] R. Lazarsfeld, *Positivity in algebraic geometry. II*, volume 49, (2004), Springer-Verlag, xviii+385.

[8] J. Lipman, *Rational singularities, with applications to algebraic surfaces and unique factorization*, Inst. Hautes Études Sci. Publ. Math. **36** (1969) 195–279.

[9] D. Naie, *Mixed multiplier ideals and the irregularity of abelian coverings of smooth projective surfaces*, Expo. Math. **31** (2013), 40–72.

Deptartament de Matemàtiques, Universitat Politècnica de Catalunya, Av. Diagonal 647, Barcelona 08028, Spain

E-mail address: Maria.Alberich@upc.edu, Josep.Alvarez@upc.edu

Institut für Mathematik, Martin-Luther-Universität Halle-Wittenberg, 06099 Halle (S.), Germany

E-mail address: ferran.dachs-cadefau@mathematik.uni-halle.de

Institut für Algebraische Geometrie, Leibniz Universität Hannover, Welfengarten 1, 30167 Hannover, Germany

E-mail address: gonzalez@math.uni-hannover.de

Monografías de la Real Academia de Ciencias. Zaragoza. **43:** 31–34, (2018).
ISSN: 1132-6360

LOWER BOUNDS OF DISTANCES BETWEEN ALGEBRAIC SURFACES AND SPACE CURVES.

JUAN GERARDO ALCÁZAR AND CARLOS HERMOSO

Abstract. We present on-going work to compute lower bounds of distances between an implicit algebraic surface, and a space algebraic curve. The main idea is to use the *level surfaces* of the polynomial defining the surface: one computes the level surface of the polynomial which first intersects the curve, and then the lower bound is computed as the distance between such level surface, and the original surface. The idea is useful to find lower bounds of distances in situations involving some simple surfaces which are, however, widely used in Computer Aided Geometric Design, like ellipsoids, surfaces of revolution, or cylindrical surfaces.

Introduction

The computation of the distance between two objects in space has been addressed in fields like Robotics, Computer Aided Geometric Design or Pattern Recognition, to quote just a few. In Robotics or Computer Aided Geometric Design the problem is important in order to detect collisions; in Pattern Recognition, it is related to the question of measuring the closeness between two objects, in order to compare them. Sometimes, the distance used is the usual Euclidean distance (see [4] and other references in this paper), while in other situations it is the Hausdorff distance that is used (see [2, 5] and other references therein).

In our case, we consider the problem of computing the usual Euclidean distance, or rather a lower bound of this distance, between an implicit algebraic surface and a space algebraic curve. In order to compute the distance exactly, one might use Lagrange multipliers; in turn, this leads to a polynomial system that can be solved, for instance, using Gröbner bases. However, in practice this approach works only when the surface is really simple: it works with quadrics, for instance, but the system can get too complicated even when we move to tori.

Here we will explore an alternative, based on the notion of *level surface*, that allows to compute a lower bound of the distance between the considered objects in certain cases. Notice that in problems concerning collisions, for instance, having a lower bound of the distance is still useful, since it allows us to certify that the objects are not colliding. At the moment, the method works only for certain types of surfaces, namely ellipsoids, bounded surfaces of revolution (which includes tori) and cylindrical surfaces; the extension to other types of surfaces is currently on-going work.

Acknowledgements. Juan G. Alcázar is Supported by the Spanish "Ministerio de Economía y Competitividad" under the project MTM2017-88796-P. Juan G. Alcázar and Carlos Hermoso are members of the Research Group ASYNACS (Ref. CCEE2011/R34).

1. Main idea.

Let S be an algebraic surface implicitly defined by $F(x, y, z) = 0$, and let $\mathcal{C}$ be a space algebraic curve. We will assume that $\mathcal{C}$ is defined by means of a rational parametrization $\mathbf{x}(t) = (x(t), y(t), z(t))$; nevertheless, the idea can be generalized to the case of implicit algebraic space curves as well, at the price of less efficiency. The *minimum distance* $\mathbf{d}_{\min}(S, \mathcal{C})$, or $\mathbf{d}_{\min}$ for short, is defined as

$$\mathbf{d}_{\min}(S, \mathcal{C}) = \min\{d(p_1, p_2) | p_1 \in S, p_2 \in \mathcal{C}\},$$

where $d(p_1, p_2)$ represents the Euclidean distance between two points $p_1, p_2 \in \mathbb{R}^3$. Whenever $\mathbf{d}_{\min} \neq 0$, this distance is achieved as the distance between two points $\mathbf{p}_1 \in S$ and $\mathbf{p}_2 \in \mathcal{C}$, called the *footpoints*. Observe that $\mathbf{d}_{\min} = 0$ when $S \cap \mathcal{C} \neq \emptyset$, but not only: if $\mathcal{C}$ approaches S asymptotically, we have $\mathbf{d}_{\min} = 0$ as well.

Under the assumption that $\mathbf{d}_{\min} \neq 0$, our goal is not to find $\mathbf{d}_{\min}$ itself, but a lower nonzero bound $\mathbf{d}^\star$, so that $\mathbf{d}_{\min} \geq \mathbf{d}^\star > 0$. The main idea of our approach is to use *level surfaces*: the level surfaces of $F(x, y, z)$ are the surfaces $F(x, y, z) = k$, for $k \in \mathbb{R}$. Now supposing that S and $\mathcal{C}$ are disjoint, one can always assume that $\mathcal{C}$ lies in the region of space where $F(x, y, z) > 0$; indeed, otherwise it is enough to take $-F$, instead of F, as the implicit equation of S. Then while $F(x, y, z) = 0$ and $\mathcal{C}$ do not have any point in common, there must exist a minimum $\mathbf{k} > 0$ such that $F(x, y, z) = \mathbf{k}$ and $\mathcal{C}$ *do* have at least one common point, which is either a singular point of S or $\mathcal{C}$, or a point where $\mathcal{C}$ and S are tangent. Furthermore, the value of $\mathbf{k}$ can be computed as the smallest positive root of

$$h(k) = \mathrm{Res}_t(G, G_t), \tag{1}$$

where $G(t, k) = F(x(t), y(t), z(t)) - k$. Calling $\mathbf{d}^\star$ to the distance between the surfaces $F(x, y, z) = 0$ and $F(x, y, z) = \mathbf{k}$, which are two level surfaces of the same polynomial (F), we have the following result.

Theorem 1.1. $\mathbf{d}_{min} \geq \mathbf{d}^\star$.

Therefore, the lower bound $\mathbf{d}^\star$ is equal to the distance between two surfaces, namely $F(x, y, z) = 0$ and its level surface $F(x, y, z) = \mathbf{k}$. Whenever the distance between them is not zero, such distance can be computed with the algorithm in [4]. However, in certain cases, we can do much better; we address this in the next section.

Fig. 1 illustrates the above idea in a planar version of the problem, namely the computation of the lower bound of the distance between two planar curves $\mathcal{C}_1, \mathcal{C}_2$, in this case a lemniscate and a circle. Fig. 1 represents both $\mathcal{C}_1, \mathcal{C}_2$ in red color, jointly with several level curves of the lemniscate, in blue color and black color; the footpoints $\mathbf{p}_1, \mathbf{p}_2$ are also represented. The black level curve with dashed-dotted line corresponds to $\mathbf{k}$; one can check that it is tangent to the circle. The black level curve in solid line corresponds to the level curve $f_1(x, y) = \mathbf{p}_2$, where $f_1(x, y)$ represents the implicit equation of the lemniscate. The minimum distance $\mathbf{d}_{\min}$ is the length of the red segment, plotted in dashed line. The value $\mathbf{d}^\star$ is the length of the blue segment, plotted in dashed line.

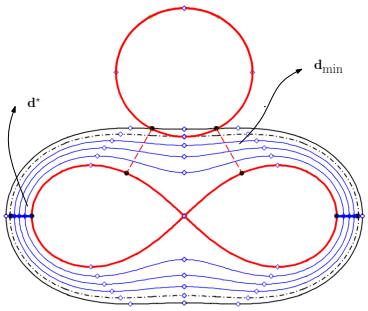


FIGURE 1. A circle and a lemniscate.

2. Distance between the level surfaces of a same surface: some interesting cases.

For certain surfaces, we can simplify the computation of $\mathbf{d}^\star$, or even easily compute it. The first type of surface where we can do this is ellipsoids; the following result can be proven by using Lagrange multipliers.

Theorem 2.1. *Let S be an ellipsoid whose implicit equation is $F(x,y,z) = \frac{x^2}{a^2}+\frac{y^2}{b^2}+\frac{z^2}{c^2}-1 = 0$, and let $\alpha = min\{a,b,c\}$. Then $\mathbf{d}^\star = \alpha\cdot(\sqrt{1+\mathbf{k}}-1)$.*

It is interesting to observe that one cannot produce a similar result for non-bounded quadrics, other than elliptic or circular cylinders; the reason is that in the other cases, $F(x,y,z) = 0$ and $F(x,y,z) = \mathbf{k}$ approach asymptotically, so that the distance between them is zero even though they do not intersect. This is the space version of a phenomenon already identified in the planar case (see [3]).

The second type of surface where we can simplify the computation of $\mathbf{d}^\star$, is surfaces of revolution. One can prove that if S is a surface of revolution about an axis $\mathcal{A}$, the level surfaces of S are also surfaces of revolution about the same axis. Based on this, one can prove the following result.

Theorem 2.2. *Let S be a surface of revolution defined by $F(x,y,z) = 0$, let $S_\mathbf{k}$ be the level surface $F(x,y,z) = \mathbf{k}$, and let $\mathcal{A}$ be the (common) axis of revolution of S and $S_\mathbf{k}$. Then $\mathbf{d}^\star$ is equal to the distance between the directrix curves $\mathcal{D},\mathcal{D}_\mathbf{k}$ of $S, S_\mathbf{k}$ respectively, obtained by intersecting $S, S_\mathbf{k}$ with a same plane Π containing $\mathcal{A}$.*

This way, we can reduce the problem from $\mathbb{R}^3$ to $\mathbb{R}^2$, which is less costly. In order to solve the problem in $\mathbb{R}^2$, one can adapt the algorithm in [4]. Additionally, when S is a torus one can prove the following result.

Corollary 2.3. *Let S be the torus of equation $F(x,y,z) = (x^2+y^2+z^2+R^2-r^2)^2 - 4R^2(x^2+y^2) = 0$, with $r<R$. Then $\mathbf{d}^\star = \left|\sqrt{\sqrt{4R^2r^2+\mathbf{k}}+R^2+r^2}-R-r\right|$.*

The third type of surface where we can simplify the computation of $\mathbf{d}^\star$ is cylindrical surfaces, where we can also reduce the problem from $\mathbb{R}^3$ to $\mathbb{R}^2$.

Theorem 2.4. *Let S be a cylindrical surface whose rulings are parallel to $\vec{v}$, and let $S_{\mathbf{k}}$ be the level surface of S corresponding to $\mathbf{k}$. Then $\mathbf{d}^\star$ is the distance between the planar curves $\mathcal{C}, \mathcal{C}_{\mathbf{k}}$ obtained by intersecting $S, S_{\mathbf{k}}$ with a plane Π normal to $\vec{v}$.*

Corollary 2.5. *Let S be an elliptic cylinder, of equation $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$, and let $\alpha = min\{a, b\}$. Then $\mathbf{d}^\star = \alpha \cdot (\sqrt{1+\mathbf{k}} - 1)$.*

The following table provides distances $\mathbf{d}$ and bounds $\mathbf{d}^\star$ for the distances between some surfaces and curves; we also provide the timings $t, t^\star$ for computing $\mathbf{d}, \mathbf{d}^\star$, and the maximum degree of the parametrization of the curve, i.e. the maximum degree of the numerators and denominators of the components. In all the cases, $t^\star < t$; furthermore, in the case of the torus we fail to compute the exact distance (computation time exceeded 300 seconds). Additionally, the parametrizations used for the curves are dense polynomials, randomly generated. The computations have been carried out with `Maple` 18.

	Surface	degree($\mathcal{C}$)	$\mathbf{d}^\star$	$t^\star$	$\mathbf{d}$	t
$(S_1, \mathcal{C}_1)$	ellipsoid	10	3.670	**0.171**	5.040	0.562
$(S_2, \mathcal{C}_1)$	elliptic cylinder	10	3.640	**0.156**	4.204	0.312
$(S_1, \mathcal{C}_2)$	ellipsoid	25	1.125	**0.453**	1.231	1.170
$(S_2, \mathcal{C}_2)$	elliptic cylinder	25	0.179	**1.170**	0.200	1.560
$(S_6, \mathcal{C}_4)$	torus	15	5.644	**2.028**	$\star$	> 300

Some last observations:

- With some technicalities, Theorem 2.1 and Corollary 2.5 can be generalized to ellipsoids and cylinders in generic position by making use of the matrix defining the quadric in each case. Similarly, Corollary 2.3 can be generalized to tori in generic position whenever the axis of revolution is computed [1].
- The method can be generalized to the implicit case, using Gröbner bases instead of resultants.

References

[1] Alcázar J.G., Goldman R. (2017), *Detecting when an implicit equation or a rational parametrization defines a conical or cylindrical surface, or a surface of revolution*, IEEE Transactions on Visualization and Computer Graphics Vol. 23, Issue 12, pp. 2550-59.

[2] Barton M., Hanniel I., Elber G., Kim M-S. (2010), *Precise Hausdorff Distance Computation between Polygonal Meshes*, Computer Aided Geometric Design Vol. 27, Issue 8, pp. 580–591.

[3] Blasco A., Pérez-Díaz S. (2014), *Asymptotes and Perfect Curves*, Computer Aided Geometric Design, Vol. 31, Issue 2, pp. 81-96.

[4] Chen X.D., Yong J-H., Zheng G-Q., Paul J-C., Sun J-G. (2006), *Computing minimum distance between two implicit algebraic surfaces*, Computer Aided Design, Vol. 38 (10), pp. 1053-1061.

[5] Rueda S., Sendra J.R., Sendra J. (2014), *Bounding and Estimating the Hausdorff distance between real space algebraic curves*, Computer Aided Geometric Design Vol. 31, Issue 34, pp. 182–198.

Departamento de Física y Matemáticas, Universidad de Alcalá, E-28871 Madrid, Spain
E-mail address: `juange.alcazar@uah.es`

Departamento de Física y Matemáticas, Universidad de Alcalá, E-28871 Madrid, Spain
E-mail address: `carlos.hermoso@uah.es`

Monografías de la Real Academia de Ciencias. Zaragoza. **43:** 35–38, (2018).
ISSN: 1132-6360

COMPUTING SYMMETRIES OF RULED RATIONAL SURFACES.

JUAN GERARDO ALCÁZAR AND EMILY QUINTERO

Abstract. We present an algorithm to compute the symmetries of a ruled surface, defined by means of a rational parametrization. The algorithm proceeds by reducing the problem to the parameter space, taking advantage of the fact that any symmetry of the surface corresponds to a birational transformation in the parameter space whose structure can be predicted.

Introduction

Symmetries of objects in 3-space are essential to describe their geometry. Additionally, knowing the symmetries of an object is also interesting from the point of view of applications because we can save time and memory space when storing shapes, and gain accuracy when reconstructing shapes from data. Because of this, the problem of computing symmetries is classical in fields like Computer Vision or Computer Aided Geometric Design, and very diverse techniques (see for instance the Introduction of the paper [2]), from Statistics to Harmonic or Spectral Analysis, have been used. However, in these contexts quite often the object to be analyzed has no structure, and may even be fuzzy up to a certain extent; for this reason, the algorithms for computing symmetries in the literature of these applied fields are approximate and numeric at heart.

In our case, we work with a symbolic object with a strong structure, namely a ruled surface defined by means of a rational parametrization, and we want to provide a symbolic algorithm to find its symmetries. In order to do this, we start from ideas already used in the curve case (see for instance [3]) and in the case of polynomially parametrized surfaces [2]. Essentially, in these papers we used the fact that any symmetry f of the object to be studied has a corresponding transformation φ in the parameter space, that inherits some of the properties of the symmetry it is associated with; computing the associated transformation φ leads, in turn, to the symmetry f itself. However, in order to find φ, first one needs to guess the structure of φ. This is easy to do for curves, but in general not for surfaces, and requires to make use of the properties of the surface (in our case, of the fact that it is ruled).

Acknowledgements. We are indebted to Carlos Hermoso and Jorge Caravantes for many discussions on the problem. Emily Quintero is financed by a grant of the Carolina Foundation. Juan G. Alcázar is Supported by the Spanish "Ministerio de Economía y Competitividad" under the project MTM2017-88796-P and a member of the Research Group ASYNACS (Ref. CCEE2011/R34).

1. Main ideas and results.

Let S be a ruled surface defined by means of a rational parametrization

$$\boldsymbol{x}(t,s) = \boldsymbol{p}(t) + s\boldsymbol{q}(t). \tag{1}$$

We will assume that $\boldsymbol{x}(t,s)$ is *proper*, i.e. generically injective, and, which is crucial for our approach, that $\boldsymbol{q}(t)$ is polynomially parametrized. Observe that we can always safely assume this last condition: indeed, for any polynomial $\mu(t)$ the two parametrizations $\boldsymbol{x}_1(t,s) = \boldsymbol{p}(t) + s\tilde{\boldsymbol{q}}(t)$ and $\boldsymbol{x}_2(t,s) = \boldsymbol{p}(t) + s\mu(t)\tilde{\boldsymbol{q}}(t)$ define the same ruled surface, since the rulings of both surfaces coincide. Thus, if $\boldsymbol{q}(t)$ is rational, we can multiply $\boldsymbol{q}(t)$ by an appropriate factor to make it polynomial; replacing the old $\boldsymbol{q}(t)$ by the new one, we get the same surface; furthermore, one can prove that this can be done without losing the properness of $\boldsymbol{x}(t,s)$.

An affine mapping $f : \mathbb{R}^3 \to \mathbb{R}^3$, where $f(x) = \mathbf{Q}x + \boldsymbol{b}$, $\mathbf{Q} \in \mathbb{R}^{3\times 3}$, $\boldsymbol{b} \in \mathbb{R}^3$, is a *symmetry* of S if f is an orthogonal transformation such that $f(S) = S$. Symmetries include classical symmetries, i.e. symmetries with respect to a plane (planar symmetries), with respect to a line (axial symmetries), with respect to a point (central symmetries), and rotational symmetries (rotations leaving S invariant). Since $\boldsymbol{x}$ is a proper parametrization, $\boldsymbol{x}^{-1}$ exists and we have the following diagram

$$\begin{array}{ccc} S & \xrightarrow{\ f\ } & S \\ {\scriptstyle \boldsymbol{x}}\uparrow & & \uparrow{\scriptstyle \boldsymbol{x}} \\ \mathbb{R}^2 & \xrightarrow[\ \varphi\ ]{} & \mathbb{R}^2 \end{array} \tag{2}$$

Here, φ is a birational transformation which makes the diagram commutative, so $f \circ \boldsymbol{x} = \boldsymbol{x} \circ \varphi$. Since $f(x) = \mathbf{Q}x + \boldsymbol{b}$, and writing $\varphi(t,s) = (\varphi_1(t,s), \varphi_2(t,s))$, we get

$$\mathbf{Q} \cdot \boldsymbol{x}(t,s) + \boldsymbol{b} = \boldsymbol{x}(\varphi_1(t,s), \varphi_2(t,s)). \tag{3}$$

In the case of symmetries of curves, i.e. when $\boldsymbol{x} : \mathbb{R} \to \mathbb{R}^d$, one has an analogous commutative diagram with $\varphi : \mathbb{R} \to \mathbb{R}$. For curves, the fact that φ is a birational transformation of the real line immediately implies that φ is a Möbius transformation, so that the structure of φ is known. In our case, however, φ is a birational transformation of the plane, i.e. a *Cremona* transformation. But unlike birational transformations of the line, Cremona transformations do not have a closed form. Thus, in order to get a clue on how φ looks like, we need to make use of the properties of the surface S; in this case, of the fact that S is ruled. The next result provides a first result in this direction. The theorem exploits the fact that any symmetry of S sends rulings to rulings, and the observation that the rulings are parametrized as $\boldsymbol{x}(t_0, s)$, with t_0 a constant; the rest of the theorem follows from Eq. (3). Additionally, here we need to exclude the case of doubly-ruled surfaces; it is well-known that these surfaces are planes, hyperbolic paraboloids and single-sheeted hyperboloids[1].

[1]These quadrics can be detected using [1], and their symmetries can be easily computed after from the matrix associated with the implicit equation of the surface, which is easy to find.

Theorem 1.1. *Let S be a rational ruled surface properly parametrized by $\boldsymbol{x}(t,s) = \boldsymbol{p}(t) + s\boldsymbol{q}(t)$, which is not doubly ruled. Then*

$$\varphi(t,s) = (\psi(t), b(t)\cdot s + a(t)), \tag{4}$$

where $\psi(t) = (\alpha t + \beta)/(\gamma t + \delta)$ is a Möbius transformation and $a(t), b(t)$ are rational functions.

When we substitute the $\varphi(t,s)$ of Eq. (4) into Eq. (3), we obtain

$$\mathbf{Q}\cdot\boldsymbol{q}(t) = b(t)\cdot\boldsymbol{q}(\psi(t)). \tag{5}$$

Additionally, since $\mathbf{Q}$ is an orthogonal matrix, we get

$$\|\boldsymbol{q}(t)\|^2 = b^2(t)\cdot\|\boldsymbol{q}(\psi(t))\|^2, \tag{6}$$

where $\|\cdot\|$ represents the usual Euclidean norm. Since $\boldsymbol{q}(t)$ is a polynomial parametrization, we deduce that the right hand-side of (6) must be a polynomial as well, and must have the same degree as $\|\boldsymbol{q}(t)\|^2$. Taking all these observations into account, one can prove the following result on the factor $b(t)$.

Lemma 1.2. *The function $b(t)$ is polynomial, and it satisfies that $b(t) = k(\gamma t + \delta)^n$, where n is the degree[2] of the parametrization $\boldsymbol{q}(t)$, $\gamma t + \delta$ is the denominator of the Möbius function $\psi(t)$ in Theorem 1.1, and k is a constant.*

Lemma (1.2), jointly with Eq. (6), provides a polynomial system for the parameters $\alpha, \beta, \gamma, \delta$ of the Möbius function $\psi(t)$, and k; additionally, since at least one of the $\alpha, \beta, \gamma, \delta$ must be nonzero, we can always pick one of them to be 1, therefore reducing the number of parameters to 4. In the case of *involutions* (i.e. whenever $f \circ f = \mathrm{Id}_{\mathbb{R}^3}$; for instance, planar symmetries, axial symmetries and central symmetries), we can do better. In that case, since $f \circ \boldsymbol{x} = \boldsymbol{x} \circ \varphi$, we obtain $\varphi \circ \varphi = \mathrm{Id}_{\mathbb{R}^2}$ as well. This adds some extra conditions on the parameters of $\psi(t)$ and $b(t)$; more precisely, one has the following two possibilities:

$$(i)\ \alpha = \delta, \beta = \gamma = 0 \text{ and } k^2 = \delta^{-2n};\ (ii)\ \alpha = -\delta, k^2(\gamma\beta + \delta^2)^n = 1.$$

Furthermore, choosing one of the parameters $\alpha, \beta, \gamma, \delta$ to be 1, we can come down to two parameters, so we need to deal with bivariate systems at most.

Once the parameters of $b(t), \psi(t)$, are computed, the matrix $\mathbf{Q}$ is computed from Eq. (5). In order to compute the symmetries $f(x) = \mathbf{Q}x + \boldsymbol{b}$ themselves, for each $\mathbf{Q}$ it remains to find the corresponding $\boldsymbol{b}$, which in turn requires to determine the function $a(t)$ in Eq. (4). For this purpose, we can go back to Eq. (3). Let us write the entries of the matrix $\mathbf{Q}$ as Q_{ij}, and let $\boldsymbol{b} = (b_1, b_2, b_3)$; also, let $p_i(t), q_i(t)$ be the components of $\boldsymbol{p}(t), \boldsymbol{q}(t)$. From Eq. (3) and taking the preceding results into account, we have

$$\mathbf{Q}\cdot\boldsymbol{p}(t) + \boldsymbol{b} = \boldsymbol{p}(\psi(t)) + a(t)\boldsymbol{q}(\psi(t)). \tag{7}$$

The above equation splits into three equations of the type

$$Q_{i1}\cdot p_1(t) + Q_{i2}\cdot p_2(t) + Q_{i3}\cdot p_3(t) + b_i = p_i(\psi(t)) + a(t)q_i(\psi(t)), \tag{8}$$

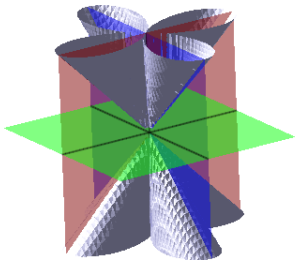
[2]That is to say, the maximum of the degrees of the components of $\boldsymbol{q}(t)$.

where $i = 1, 2, 3$. If $a(t)$ is identically zero (which happens, for instance, when S is a conical surface), evaluating Eq. (7) already yields $\boldsymbol{b}$. Otherwise, we need to examine in more detail the system provided by Eq. (7). In this system we already know the Q_{ij}, and $\psi(t)$. Now, eliminating the function $a(t)$ in the equations of Eq. (7) and evaluating at a random $t_0 \in \mathbb{R}$, we can write b_1, b_2, b_3 in terms of just one of them, say b_3. Then we can write $a(t)$ in terms of b_3, t, and impose that Eq. (3) holds identically. From here, all the symmetries of the surface can be computed. Computing the values for the parameters $\alpha, \beta, \gamma, \delta$ is the step which dominates the complexity of the whole procedure, which is polynomial [4].

For instance, consider the conical surface S parametrized by

$$\boldsymbol{x}(t, s) = (2ts(t^4 - 6t^2 + 1), s(-t^2 + 1)(t^4 - 6t^2 + 1), s(t^2 + 1)^3).$$

This surface has many symmetries, but for lack of space we will just mention its 3 planes of symmetry, which happen to coincide with the coordinate planes. The function $\varphi(t, s) = (-t, s)$, where $\alpha = -1$, $\beta = 0$, $\gamma = 0$, $\delta = 1$ and $k = 1$, corresponds to the symmetry with respect to the yz-plane. Also, $\varphi(t, s) = \left(\frac{1}{t}, s \cdot t^6\right)$ corresponds to the symmetry with respect to the xz-plane. Additionally, $\varphi(t, s) = \left(\frac{-t+1}{t+1}, \frac{-s(t+1)^6}{8}\right)$ corresponds to the symmetry with respect to the xy-plane. The symmetry planes, in red, green and blue color, are shown in the figure jointly with the surface S.



References

[1] Albrecht G. (1998), *Determination and classification of triangular quadric patches*, Computer Aided Geometric Design Vol. 15, Issue 7, pp. 675–697.

[2] Alcázar J.G., Hermoso C. (2016), *Involutions of polynomially parametrized surfaces*, Journal of Computational and Applied Mathematics Vol. 294, pp. 23–38.

[3] Alcazár J.G., Hermoso C., Muntingh G. (2015), *Symmetry detection of rational space curves from their curvature and torsion*, Computer Aided Geometric Design, Vol. 33, pp. 51–65.

[4] Brand C., Sagraloff M. (2016), *On the complexity of solving zero-dimensional polynomial systems via projection*, Proceedings ISSAC 16, pp. 151–158.

Departamento de Física y Matemáticas, Universidad de Alcalá, E-28871 Madrid, Spain
E-mail address: juange.alcazar@uah.es

Departamento de Física y Matemáticas, Universidad de Alcalá, E-28871 Madrid, Spain
E-mail address: emily.quintero@edu.uah.es

Monografías de la Real Academia de Ciencias. Zaragoza. **43:** 39–42, (2018).
ISSN: 1132-6360

REAL CANONICAL FORMS IN WARING'S PROBLEM. A CONSTRUCTIVE APPROACH

M. ANSOLA, A. DÍAZ-CANO, AND M. A. ZURRO

Abstract. In this talk, we give an explicit parametric presentation of semialgebraic neighborhoods with constant Waring real rank for typical real binary forms. Some non trivial examples will be presented. The computations were made in Maple.

1. Introduction

It is known that any real homogeneous polynomial of degree d can be decomposed as sum of r d-th powers of real linear forms. When this number r is minimal is called the Waring rank or symmetric tensor rank of the form. The aim of this work is to study Waring decompositions of homogeneous polynomials of degree d in two real variables that are stable under perturbation of their coefficients. The Waring Problem, also called Symmetric Tensor Decomposition, arises in signal and image processing, automatic control and many problems in Electrical Engineering.

We are going to present a construction for a Waring decomposition of a typical real binary form p that enables perturbative processes in the space $\mathcal{B}_d$ of real binary forms of degree d. In [4] and [5], for example, a *typical rank* r is a rank such that $\mathcal{B}_d$ contains a non-empty open set of real binary forms of rank r (for the usual topology of $\mathbb{R}^{d+1}$). We are going to work with a form p of real rank r such that there exists an open neighborhood of p (in $\mathcal{B}_d$) of constant real rank r and we will call p a *typical real form* of real rank r. Observe that r must be typical, but there exist binary forms of rank r that are not typical forms.

In [7], B. Reznick gives some new canonical representations for forms over $\mathbb{C}$. We benefit from Reznick's ideas, in particular Theorem 1.6 in [7], to obtain a polynomially encoded neighborhood of p that involve real linear forms. Theorem 2.2 have been implemented in Maple, and an explicit example is shown in section 3. With this method we can find real binary forms by perturbing a typical form p, ensuring that the real rank remains stable in a neighborhood of p. These deformations seem to be new, as far as we know.

2. Real canonical forms. The binary case

Let fix a typical real binary form $p(x,y) = \sum_{i=0}^{d} \binom{d}{i} c_i x^i y^{d-i}$ of real rank r. Then we have:

$$p(x,y) = \sum_{i=1}^{r} \lambda_i \ell_i^d \tag{1}$$

for some linear forms $\ell_i(x,y) = a_i x + b_i y$, and some real numbers λ_i. Next we present a method to give a parametric presentation of a neighborhood of $p \in \mathcal{B}_d$ of constant real rank

Second author partially supported by Spanish MTM2014-55565 and Grupo UCM 910444.
Third author partially supported by Grupo UCM 910444.

r. For that we will introduce a polynomial real function, F, that will encode the announced local presentation.

A **canonical form at** p is any polynomial $G(t_1,\dots,t_{d+1};x,y) = G(\underline{t};x,y)$ with the property that there exists a neighborhood Ω of $p \in \mathcal{B}_d$ so that for each real binary form $q(x,y)$ in Ω there exists $\underline{t} \in \mathbb{R}^{d+1}$ such that $q(x,y) = G(\underline{t};x,y)$.

Next we give a procedure to construct a canonical form at p that maintains the real rank r of p in Ω, whenever p is a typical real binary form. For complex forms, the set of binary forms of rank exactly r has non-empty interior for $r = \lfloor \frac{d}{2} \rfloor + 1$ (see [5]), so there is only one *generic rank*. However, in the real case, all ranks between $\lfloor \frac{d}{2} \rfloor + 1$ and d are typical (see [4] and [5]).

The construction. Take $m = 2r-(d+1)$. Observe that m is non negative since the rank r is typical. Now we take the linear forms $\ell_1,\dots,\ell_m$ from (1). For $j = 1,\dots,r-m$, we define the polynomials f_{m+j} by $f_{m+j}(t_{m+j},t'_{m+j}) = t_{m+j}x + t'_{m+j}y$. Next, let us consider:

$$F(\underline{z},\underline{t}\,) = \sum_{i=1}^{m} t_i \ell_i^d + \sum_{j=1}^{r-m} f_{m+j}^d - \sum_{i=0}^{d} \binom{d}{i} z_i x^i y^{d-i} = \sum_{k=0}^{d} F_k(\underline{z},\underline{t}\,) x^k y^{d-k}. \tag{2}$$

Observe that

$$\frac{\partial F}{\partial t_i} = \ell_i^d\,, \qquad \frac{\partial F}{\partial t_{m+j}} = d f_{m+j}^{d-1} x\,, \qquad \frac{\partial F}{\partial t'_{m+j}} = d f_{m+j}^{d-1} y\,, \tag{3}$$

where $i = 1,\dots,m$ and $j = 1,\dots,r-m$. Hence the polynomial mapping

$$\begin{array}{rcl} F : \mathbb{R}^{d+1} \times \mathbb{R}^{d+1} & \longrightarrow & \mathbb{R}^{d+1} \\ (\underline{z},\underline{t}\,) & \longmapsto & (F_0(\underline{z},\underline{t}\,),\dots,F_d(\underline{z},\underline{t})) \end{array} \tag{4}$$

has a Jacobian matrix at $z^\star = (c_0,\dots,c_d)$ of maximal rank. In fact, this matrix can be written as[1]

$$J_F = \left(\begin{array}{ccc|ccc} \frac{\partial F_0}{\partial z_0} & \cdots & \frac{\partial F_0}{\partial z_d} & \frac{\partial F_0}{\partial t_1} & \cdots & \frac{\partial F_0}{\partial t_{d+1}} \\ \vdots & & \vdots & \vdots & & \vdots \\ \frac{\partial F_d}{\partial z_0} & \cdots & \frac{\partial F_d}{\partial z_d} & \frac{\partial F_d}{\partial t_1} & \cdots & \frac{\partial F_d}{\partial t_{d+1}} \end{array}\right) = \left(D_{\underline{z}}F \,|\, D_{\underline{t}}F\right)\,,$$

where $(D_{\underline{z}}F)$ is a diagonal matrix with non zero entries $d_i = -\binom{d}{i-1}$, for $1 \le i \le d+1$. We decompose $D_{\underline{t}}F$ as $(M_{ab}|M_t)$, where the j-th column of M_{ab} is

$$\left(b_j^d \ \cdots \ \binom{d}{i-1} a_j^{i-1} b_j^{d+1-i} \ \cdots \ a_j^d\right)^t\,,\ 1 \le j \le m\,,$$

and each j-th column of M_t is

$$\left(0 \ \cdots \ \binom{d}{i-1} (i-1)\, t_{m+j}^{i-2} {t'}_{m+j}^{\,d+1-i} \ \cdots \ d\, t_{m+j}^{d-1}\right)^t \text{ for } j \text{ odd},$$

$$\text{and} \qquad \left(d\, {t'}_{m+j}^{\,d-1} \ \cdots \ \binom{d}{i-1} (d-i+1)\, t_{m+j}^{i-1} {t'}_{m+j}^{\,d-i} \ \cdots \ 0\right)^t \text{ for } j \text{ even},$$

[1]For convenience, we rewrite $(t_1,\dots,t_m,t_{m+1},t'_{m+1},\dots,t_r,t'_r)$ as $(t_1,\dots,t_{d+1})$.

because of (3). Thanks to the structure of this Jacobian matrix, the determinant of $D_{\underline{t}}F$ can be factorized as

$$|D_{\underline{t}}F| = k \prod_{\substack{i=1,\dots,m\\ i<j}} (a_ib_j - a_jb_i) \prod_{\substack{i=1,\dots,m\\ m+1\le j\le r-m}} (a_it'_j - b_it_j)^2 \prod_{\substack{i=m+1,\dots,r-m\\ i<j}} (t_it'_j - t_jt'_i)^4.$$

Therefore, $|D_{\underline{t}}F(z^\star, t^\star)| \neq 0$, where $t^\star = (\lambda_1, \dots, \lambda_m, a_{m+1}, b_{m+1}, \dots, a_r, b_r)$, and the Jacobian matrix has maximal rank in that point. Moreover $F(z^\star, t^\star) = 0$. By the Implicit Function Theorem (see, for example, [6], page 44), there exists an open semialgebraic neighborhood of $\underline{z}^\star$ in $\mathbb{R}^{d+1}$, Ω, and a Nash mapping $g : \Omega \ni \underline{z} \longrightarrow (g_1(\underline{z}), \dots, g_{d+1}(\underline{z})) \in \mathbb{R}^{d+1}$ such that $F(\underline{z}, g(\underline{z})) = 0$ for each $\underline{z} \in \Omega$.

Remark 2.1. Observe that F_k is not a linear function in t_j in general. Moreover, $t_j = g_j(\underline{z})$ can be seen as element of the ring of algebraic series (see [1] and [2]).

The above construction gives the proof of the following result.

Theorem 2.2. *Let r be a positive integer such that $\lfloor \frac{d}{2} \rfloor + 1 \le r \le d$. Let consider $p(x, y)$ a real typical form of real rank r, fix a real Waring decomposition of p as in* (1)*, and take $m = 2r - (d + 1)$. Then, there exists an open neighborhood Ω of $(c_0, \dots, c_d)$ in $\mathbb{R}^{d+1}$ such that for $\underline{z} = (z_0, \dots, z_d) \in \Omega$, we have*

$$q(x,y) = \sum_{i=0}^{d} \binom{d}{i} z_i x^i y^{d-i} = \sum_{i=1}^{m} t_i \ell_i^d + \sum_{j=1}^{r-m} (t_{m+j}x + t'_{m+j}y)^d = \sum_{i=1}^{m} t_i \ell_i^d + \sum_{j=1}^{r-m} f_{m+j}^d \tag{5}$$

with $t_i = g_i(\underline{z})$ Nash functions and $\{\ell_j\}_{j=1}^m \cup \{f_{m+j}\}_{j=1}^{r-m}$ pairwise non-proportional linear forms with real coefficients.

Remark 2.3. The function (4) given in the above construction guarantees the existence of a canonical form at p for a typical form that keeps stable the Waring's real rank in a neighborhood of p.

3. An explicit example

Example 3.1. Let's consider $p = p(x, y) = y^4 - 5x^2y^2 + 4x^4$. It is a typical form of degree 4, with a known Waring's decomposition:

$$p = -\frac{291}{188}(x-y)^4 - \frac{397}{2484}(x+y)^4 + \frac{319}{1890}(x-2y)^4 + \left[\left(\frac{5658248}{1021545}\right)^{\frac{1}{4}} x - \frac{11}{58}\left(\frac{5658248}{1021545}\right)^{\frac{1}{4}} y\right]^4.$$

From this decomposition, following the given construction, we define

$$\begin{aligned} F(\underline{z}, \underline{t}) = \; & t_1(x-y)^4 + t_2(x+y)^4 + t_3(x-2y)^4 + (t_4x + t'_4y)^4 - \\ & -(z_0y^4 + 4z_1xy^3 + 6z_2x^2y^2 + 4z_3x^3y + z_4x^4) = \textstyle\sum_{k=0}^4 F_k(\underline{z}, \underline{t})x^k y^{d-k}. \end{aligned}$$

Now, in order to solve $F(\underline{z},\underline{t}\,)=0$, we take $t_5=t_4'=\alpha t_4$. The system $\{F_0=0,F_1=0,F_2=0\}$ is linear in t_1,t_2,t_3. Then, we obtain:

$$\begin{aligned} t_1 &= \tfrac{\alpha^2(\alpha+2)(\alpha-1)}{2}t_4^4-\tfrac{1}{2}(z_0+z_1-2z_2),\\ t_2 &= -\tfrac{\alpha^2(\alpha+2)(\alpha+1)}{6}t_4^4+\tfrac{1}{6}(z_0+3z_1+2z_2),\\ t_3 &= -\tfrac{\alpha^2(\alpha^2-1)}{12}t_4^4+\tfrac{1}{12}(z_0-z_2), \end{aligned}$$

Now, we can compute F_3 and F_4 with these values of $t_1,\ t_2,\ t_3$, and we find

$$\alpha=\alpha(\underline{z})=\frac{z_0+2z_1-z_2-2z_3}{z_1+2z_2-z_3-2z_4} \tag{6}$$

and also

$$t_4(\underline{z})^4=\frac{z_0-5z_2+4z_4}{(\alpha^2-4)(\alpha^2-1)}\ ,\quad t_5(\underline{z})=\alpha(\underline{z})t_4(\underline{z}). \tag{7}$$

We can compute these values at $\underline{z}^\star=(1,0,-5/6,0,4)$, and we obtain: $\alpha(\underline{z}^\star)=-11/58$, $t_1(\underline{z}^\star)=-\frac{291}{188}$, $t_2(\underline{z}^\star)=-\frac{397}{2484}$, $t_3(\underline{z}^\star)=\frac{319}{1890}$, and

$$t_4(\underline{z}^\star)=\left(\frac{5658248}{1021545}\right)^{\frac{1}{4}},\quad t_5(\underline{z}^\star)=-\frac{11}{58}\left(\frac{5658248}{1021545}\right)^{\frac{1}{4}}.$$

Since $t_4(\underline{z})^4$ must be positive near $\underline{z}^\star$, a suitable neighborhood Ω is given by the inequalities $|\alpha(\underline{z})|<1$ or $|\alpha(\underline{z})|>2$, because of (7). Observe that this neighborhood Ω can be described by linear functions.

Acknowledgements

We wish to thank the referees for their interesting remarks and suggestions.

References

[1] Alonso, M.E., Mora, T. and Raimondo, M., A computational model for algebraic power series. J. Pure Appl. Algebra, Vol. 77 (1992), 1-38.
[2] Alonso, M.E., Castro-Jiménez, F.J. and Hauser, H., Encoding Algebraic Power Series. Found. Comput. Math. (2017) 1-45.
[3] Ballico, E., On the typical rank of real bivariate polynomials. Linear Algebra Appl., Vol. 452, (2014) 263-269.
[4] Blekherman, G., Typical Real Ranks of Binary Forms. Found. Comput. Math., Vol. 15 (2015) 793-798.
[5] Comon, P. and Ottaviani, G., On the typical rank of real binary forms. Linear and Multilinear Algebra, Vol. 60, (6), (2012) 657-667.
[6] Łojasiewicz, S. and Zurro, M. A., Una introducción a la Geometría semi- y sub- analítica. Ed. Universidad de Valladolid (1993).
[7] Reznick, B., Some new canonical forms for polynomials. Pacific J.Math. 266(1), (2013) 185-220.

Universidad Complutense de Madrid
E-mail address: mansola@ucm.es

Universidad Complutense de Madrid. Facultad de Matemáticas.
IMI and Dpto. de Álgebra, Geometría y Topología
E-mail address: adiazcan@ucm.es

Universidad Autónoma de Madrid
E-mail address: mangeles.zurro@uam.es

Monografías de la Real Academia de Ciencias. Zaragoza. **43:** 43–46, (2018).
ISSN: 1132-6360

TOWARDS A VERIFIED SMITH NORMAL FORM ALGORITHM IN ISABELLE/HOL

JOSÉ DIVASÓN AND JESÚS ARANSAY

Abstract. In this note we report on a project to get a verified program to compute the Smith normal form of a matrix in Isabelle/HOL. The presented approach tries to tackle the problems that arise in an environment without dependent types as well as we try to reuse previous developments, keeping also the focus of the formalization on its full generality.

Introduction

A matrix over a Bézout domain is in Smith normal form, from here on *SNF*, if its diagonal elements α_i satisfy $\alpha_i|\alpha_{i+1}$ and the rest of elements of the matrix are zeros. Over such a structure, there exists an algorithm to transform a matrix A into its corresponding SNF S by means of invertible matrices, i.e., there exist invertible matrices P and Q such that $S = PAQ$. This well-known canonical form possesses many applications, such as the computation of determinants and solving a system of diophantine equations. It is also useful for computing the homology of a chain complex and of a simplicial complex. More generally, it is useful to compute persistent homology, which can be applied to process big volume of data. Thus, it is interesting to apply formal methods and get a verified algorithm to compute this form, trying to minimize bugs and errors that can cause important losses. In this work, we present a work in progress to formalize the SNF in Isabelle/HOL.

Preliminaries

Isabelle is a generic theorem prover which has been instantiated to support different object-logics. The most widespread of them is HOL. Isabelle's version of HOL (usually called Isabelle/HOL) corresponds to Church's simple type theory extended with polymorphism, Haskell-style type classes and type definitions. The HOL Analysis library (from here on, *HA*) is a huge Isabelle library which contains many theoretical results in mathematical fields such as Analysis, Topology and Linear Algebra. Its vector representation is based on the ideas by Harrison [6], where a vector $v \in \mathbb{R}^n$ is represented as a function of type $\alpha \Rightarrow \mathbb{R}$ where α is a type with n elements, that is, a finite type of cardinality n. Similarly a matrix $A \in \mathbb{R}^{n\times m}$ is represented by a function of type $\alpha \Rightarrow \beta \Rightarrow \mathbb{R}$ where β is a finite type with m elements. However, a subject that had not been explored either in the HA library (or any HOL prover) was to provide an executable implementation of such a representation. To this end, in our previous work [1] we developed a framework where algorithms over matrices can be formalized, executed, refined, and coupled with their mathematical meaning. The basic idea of the framework comes from the data refinement strategy: soundness of algorithms

This work is funded by the Spanish projects MTM2014-54151-P and MTM2017-88804-P.

should be proven in an abstract type, where proofs are feasible but does not achieve a good performance, or even prevent code execution. Execution is carried out in other more efficient concrete structure, which is connected to the abstract representation by means of morphisms. In our case, we provide a refinement to immutable arrays, which correspond to *Vector* in SML and to *IArray.array* in Haskell. This representation defines polymorphic vectors, immutable sequences with constant-time access, and thus, an efficient representation for vectors and matrices. Code from the formalizations using this framework can be exported to functional languages, such as SML and Haskell, by means of the Isabelle code generation tool. This framework was successfully applied to the formalization of various linear algebra algorithms, such as the Gauss-Jordan algorithm [1] and the echelon form [2]. However, there is no formalization of the SNF or any result involving homology, neither using this framework nor any other representation in Isabelle. It does exist a formalization in Coq [3].

Towars a verified computation of the Smith Normal Form

Most of the algorithms to compute the SNF of a matrix are based on submatrices [9]. Unfortunately, submatrices are a delicate issue in the HA library. Let A be an $n \times n$ integer matrix. Such a matrix A would be modeled in the HA library by means of a function of type $\alpha \Rightarrow \alpha \Rightarrow \mathbb{Z}$, where α is a finite type of cardinality equal to n. Let us say that we want to obtain the $(n-1) \times (n-1)$ submatrix from the first element of A, that is, getting rid of the last row and last column. Since Isabelle does not feature dependent types, we cannot use the size of the matrix in the definition. Indeed, we cannot generate a type of the desired cardinality, that is, it is not possible to define a function of type $\beta \Rightarrow \beta \Rightarrow \mathbb{Z}$ imposing cardinality of β to be $n-1$. To sum up, the output type of the function submatrix clearly depends on the input term (the original matrix), which is not expressible in Isabelle/HOL as it does not allow dependent types. A possible workaround is to complete with zeros the deleted elements, and model the output also as a matrix of the same dimension, that is, a function of type $\alpha \Rightarrow \alpha \Rightarrow \mathbb{Z}$. A similar approach of filling with zeros was already introduced by Obua on its formalization of bounds for real linear programs [8]. However, this approach has some drawbacks: we are not really representing a submatrix and internally performance will decrease, one just has to think what happens when taking a small submatrix of a very big matrix. This makes the formalization of the SNF to be harder than usual, and even if one achieves it, performance would be poor due to the overhead produced by the workaround of filling with zeros. As an alternative, we propose the following strategy.

(1) Change completely of framework and representation, and implement an algorithm to compute the SNF of a matrix in the new library developed by Thiemann and Yamada [10]. Soundness of the algorithm would be proved in it.
(2) Define in the HA library the basic concepts of homology and the definition of SNF.
(3) Connect both libraries and generate statements in both worlds, by means of the lifting and transfer package as well as the use of local type definitions [7].

Thiemann and Yamada already faced the problem of working with submatrices when formalizing Jordan normal forms of matrices, a kind of forms whose construction is done by means of block matrices. As a solution, they propose a new matrix representation, from here on *JNF*, which is indeed an abstraction of the HA representation, but flexible for dimensions. A vector $(v_0, \ldots, v_{n-1})$ is represented by a pair (n, v), where n is the dimension and v the

characteristic function (from natural numbers to the type of the elements of the vector), i.e., $v\ i = v_i$. They provide a similar representation for matrices, based on a triple (n, m, f) with the number of rows, number of columns and the characteristic function for a matrix. They prove again many properties of linear algebra and matrices based on such a representation, and they indeed connect it to immutable arrays using our libraries to be able to export efficient code. This new library is far from having all theorems presented in the HA library, but it is growing nowadays and was used successfully to provide executable algorithms for computing Jordan blocks of matrices. Our approach would consist of using this new library to formalize the SNF: there won't be problems with submatrices since they are easily supported by the library, and indeed, they are already defined in the JNF development. However, many results are present in the HA library, and indeed our framework is based on it, so formalizing the SNF with JNF framework would make it isolated. Moreover, we aim to formalize many results of homology based on the HA library, but then we could not connect it with the computable side of a formalized SNF, since it would have been done in other library. We propose the following solution: use the lifting and transfer package to connect both developments. It is relatively easy to do a proof in the HA world based on a result in JNF: from a HA-statement involving vectors or matrices, by means of transfer rules we can obtain the corresponding statement in JNF, prove it in such a world and then return the result to HA, since we already know the type dimension of the vector and matrices involved. However, the other way is not that easy and at some point it would be necessary for our development. As we have said, Isabelle does not allow dependent types. Then, after some technical work it would also be possible to transfer a statement from a JNF statement to a HA-statement, but possibly with an extra assumption in the lemmas relating a type with the dimension: $n = \mathit{CARD}(\alpha)$. One example of this can be seen in the following lemma, obtained from a development of the Berlekamp–Zassenhaus factorization algorithm for integer polynomials [5]. It just states that the output of Berlekamp's algorithm to factorize polynomials modulo a prime p is correct. Let us remark that p is demanded to be a prime number equal to the cardinality of a finite type.

assumes *finite_field_factorization'* (*ff_ops* p) $g = (c, gs)$
  and $p = \mathit{CARD}(\alpha :: \mathit{prime\_card})$ ***and*** `(* More premises *)`
shows $\mathit{unique\_factorization}_p\ f\ (c, \mathit{mset}\ fs)$

The challenge is to get rid of this premise, being substituted by ***prime*** p in that case. This was impossible before, but now we can do it by means of Isabelle's recent addition of local type definitions, a soundness extension to Isabelle/HOL's logic. Fortunately, this approach and the necessary connection between both libraries were already formalized in the mechanized proof of the Perron–Frobenius theorem [4], were some results were proven in HA, transferred to JNF representation, proved some properties there and finally *untransferred* the final result to HA. Our idea would be similar. We aim to take advantage of the best of each side: theorems and proofs involving homology would be proven in the HA-world to reuse existing results and our framework, the SNF would be defined and proved in the JNA world, where it is possible to work easily with submatrices, and finally all the results and soundness would be put together by means of the lifting and transfer package, the existing connection in the Perron–Frobenius development [4] and the use of local type definitions. This way, the homology results would be stated in the HA library whereas the SNF algorithm would be

implemented (and executed) in the JNF library, but its soundness in both worlds. Then the mathematical connection between homology and the output of the SNF would be preserved. In addition, thanks to this approach we can follow a similar strategy to our previous work of the echelon form of a matrix [2] to prove the existence of the SNF in general over any Bézout domain, and then later derive an executable algorithm parametrized by executable operations to compute Bézout coefficients. Then, our formalization would not be limited to integer matrices, but it would also allow other structures such as polynomial matrices. The idea of using functions as parameters in the algorithm is very interesting, since it could also allow us to formalize at once different versions (we impose some conditions for such parameters, but that specification can be satisfied by different implementations). For instance, we could parameterize the algorithm by a pivot function, to tackle the different ways of selecting pivots in each step. Moreover, also thanks to our framework and the connection to HA theorems, it seems to be feasible to prove the uniqueness of this normal form with the presented strategy.

Conclusions

We have presented an approach to verify the SNF in Isabelle/HOL, and then, a way to get verified algorithms to compute homology groups. Although the approach is far from being trivial and involves different techniques, it seems a feasible way to avoid the limitations of the existing libraries in an environment without dependent types. Indeed, a similar approach was successfully used in other contexts, such as the formalization of the Perron–Frobenius theorem and the Berlekamp–Zassenhaus algorithm.

References

[1] J. Aransay and J. Divasón. Formalisation in higher-order logic and code generation to functional languages of the Gauss-Jordan algorithm. *J. Funct. Program.*, 25, 2015.
[2] J. Aransay and J. Divasón. Formalisation of the computation of the echelon form of a matrix in Isabelle/HOL. *Formal Asp. Comput.*, 28(6):1005–1026, 2016.
[3] G. Cano, C. Cohen, M. Dénès, A. Mörtberg, and V. Siles. Formalized linear algebra over Elementary Divisor Rings in Coq. *Logical Methods in Computer Science*, 12(2), 2016.
[4] J. Divasón, S. J. C. Joosten, O. Kuncar, R. Thiemann, and A. Yamada. Efficient certification of complexity proofs: formalizing the Perron-Frobenius theorem. In *Proceedings of the 7th Conference on Certified Programs and Proofs*, pages 2–13, 2018.
[5] J. Divasón, S. J. C. Joosten, R. Thiemann, and A. Yamada. A formalization of the Berlekamp-Zassenhaus factorization algorithm. In *Proceedings of the 6th Conference on Certified Programs and Proofs*, pages 17–29, 2017.
[6] J. Harrison. The HOL Light Theory of Euclidean Space. *J. Autom. Reasoning*, 50(2):173 – 190, 2013.
[7] O. Kuncar and A. Popescu. From Types to Sets by Local Type Definitions in Higher-Order Logic. In *Proceedings of the 7th Interactive Theorem Proving International Conference*, pages 200–218, 2016.
[8] S. Obua. Proving Bounds for Real Linear Programs in Isabelle/HOL. In *Proceedings of the Theorem Proving in Higher Order Logics International Conference*, pages 227–244, 2005.
[9] A. Storjohann. *Algorithms for Matrix Canonical Forms*. PhD thesis, Swiss Federal Institute of Technology Zurich, 2000.
[10] R. Thiemann and A. Yamada. Formalizing Jordan normal forms in Isabelle/HOL. In *Proceedings of the 5th Conference on Certified Programs and Proofs*, pages 88–99, 2016.

Universidad de La Rioja, Edificio CCT – C/Madre de Dios 53, 26006 Logroño, La Rioja, Spain.
E-mail address: {jose.divason,jesus-maria.aransay}@unirioja.es

Monografías de la Real Academia de Ciencias. Zaragoza. **43:** 47–50, (2018).
ISSN: 1132-6360

DME: A PROPOSAL FOR A QUANTUM RESISTANT ENCRYPTION SCHEME BASED ON POLYNOMIAL MAPPINGS.

MARTÍN AVENDAÑO GONZÁLEZ, IGNACIO LUENGO VELASCO,
AND MIGUEL ÁNGEL MARCO BUZUNÁRIZ

Abstract. We present a very high degree multivariate cryptosystem. This means that it consists on polynomial maps over finite fields. The encryption map is the composition of alternated linear maps and matrix exponentiations, whereas the individual elementary maps form the private key. This system allows for reasonably short keys, and it does not rely on the hardness of discrete logarithm or integer factorization, which makes it a suitable candidate for a post-quantum use case.

Introduction

All widely used public key cryptosystems rely on the computational hardness of either the integer factorization (RSA) or the discrete logarithm on Galois fields (El Gamal) or elliptic curves (ECDH). All these problems can be reduced to computing the period of a discrete function, which can be solved in polynomial time by a quantum computer running Shor's algorithm [6].

In 2016 the NIST called for candidates for standardization of quantum safe (postquantum) public key schemes. The open call ended on November 2017 with 83 proposal of 17 countries most of them based on lattices, error correcting codes and (quadratic) multivariate systems.

The multivariate schemes consist in a series of polynomial maps over finite fields that can be easily reversed individually, whose composition is hard to reverse without knowing the elementary components.

In this talk, we describe the multivariate scheme DME that we presented to the NIST based on a new construction of the central maps. In this scheme, the elementary pieces are three linear maps, alternated with matrix exponentiations. The resulting composition is a map with very high degree and a moderate number of monomials.

1. Matrix exponentiations

Let $\mathbb{F}$ be a finite field of $q = p^s$ elements, where p is a prime integer. We have that the map

$$\begin{array}{ccc} \mathbb{F} & \longrightarrow & \mathbb{F} \\ x & \longmapsto & x^{q-1} \end{array}$$

maps every element in $\mathbb{F}^*$ to 1.

Definition 1.1. Given an $n \times m$ matrix $M = (m_{i,j})$ with integer coefficients, the map

$$\begin{array}{rcl}(\mathbb{F}^*)^n & \longrightarrow & (\mathbb{F}^*)^m \\ (x_1,\ldots,x_n) & \longmapsto & (\prod_{i=1}^n x_i^{m_{i,1}},\ldots,\prod_{i=1}^n x_i^{m_{i,m}})\end{array}$$

is called a *matrix exponentiation map.*

It is easy to see that the composition of two such matrix exponentiation maps is again a matrix exponentiation, given by the product of the corresponding matrices. One way to see it is to notice that, taking discrete logarithms, matrix exponentiations become linear maps given by the same matrices.

In particular, combining the composition property with Lagrange's theorem, we obtain the following

Lemma 1.2. *Given two $n \times n$ matrices with integer coefficients $M = (m_{i,j})$, $N = (n_{i,j})$ such that $M \cdot N$ is the identity matrix modulo $q-1$, the corresponding matrix exponentiations are inverse mappings on $(\mathbb{F} \setminus \{0\})^n$.*

Proof. Since the composition matrix is the identity modulo $(q-1)$, the j-th entry of the composition map will be of the form $x_j \cdot (x_1^{a_1^j(q-1)} \cdots x_n^{a_n^j(q-1)})$ for some integers $a_1^j, \ldots, a_n^j$. By Fermat's little theorem, if all the x_i's are in $\mathbb{F}^*$, this expression will be equal to x_j. □

2. Construction of the encryption map

Fix two integers $m > n$, and a finite field $\mathbb{F}_q$ of characteristic p. If we fix two irreducible polynomials over $\mathbb{F}_q$ of degrees m and n, we get isomorphisms $(\mathbb{F}_q)^m \cong \mathbb{F}_{q^m}$ and $(\mathbb{F}_q)^n \cong \mathbb{F}_{q^n}$, which allows us to see $(\mathbb{F}_q)^{nm}$, $(\mathbb{F}_{q^m})^n$ and $(\mathbb{F}_{q^n})^m$ as isomorphic $\mathbb{F}_q$-vector spaces. In the following, we will implicitly use these isomorphisms.

The public key of our cryptosystem is a map $F : \mathbb{F}_q^{nm} \to \mathbb{F}_q^{nm}$ obtained as composition of five maps, $F = L_3 \circ G_2 \circ L_2 \circ G_1 \circ L_1$, according to the diagram:

$$\mathbb{F}_q^{nm} \xrightarrow{L_1} (\mathbb{F}_{q^n})^m \xrightarrow{G_1} (\mathbb{F}_{q^n})^m \xrightarrow{L_2} (\mathbb{F}_{q^m})^n \xrightarrow{G_2} (\mathbb{F}_{q^m})^n \xrightarrow{L_3} \mathbb{F}_q^{mn}$$

$$\mathbb{F}_q^{nm} \xrightarrow{\quad F \quad} \mathbb{F}_q^{mn}$$

The maps L_1, L_2 and L_3 are $\mathbb{F}_q$-linear isomorphism and L_1 satisfies that for every $x \in (\mathbb{F}_q^n \setminus \{0\})^m$, $L_1(x) \in (\mathbb{F}_q^n \setminus \{0\})^m$. The map L_2 is designed to verify the condition:

$$\forall y \in (\mathbb{F}_q^n \setminus \{0\})^m,\ L_2(y) \in (\mathbb{F}_q^m \setminus \{0\})^n.$$

The maps G_1 and G_2 are invertible monomial maps (in the sense of Lemma 1.2) whose entries are powers of p. With all the above conditions it is clear that F is injective in $(\mathbb{F}_q^n \setminus 0)^m$ and the components of F and F^{-1} are given by polynomials in $\mathbb{F}_q[x_1, \ldots, x_{mn}]$. The maps G_1 and G_2 are chosen in such a way that the polynomial F has few monomials and the polynomial F^{-1} has a huge number of monomials. More precisely, the map F is a composition of the following steps:

- An invertible linear map $L_1 : (\mathbb{F}_q)^{nm} \longrightarrow (\mathbb{F}_q)^{nm}$ given by a matrix that is the diagonal sum of m $n \times n$ boxes.

- A matrix exponentiation map $G_1 : (\mathbb{F}_{q^n})^m \longrightarrow (\mathbb{F}_{q^n})^m$ given by an invertible $m \times m$ matrix over $\mathbb{Z}/(q^n - 1)\mathbb{Z}$ that has exactly two nonzero entries in each row and each column; and such that the nonzero entries are always powers of p.
- An invertible linear map $L_2 : (\mathbb{F}_q)^{nm} \longrightarrow (\mathbb{F}_q)^{nm}$ given by a matrix that is the diagonal sum of n $m \times m$ boxes (maybe composed with a permutation matrix).
- A matrix exponentiation map $G_2 : (\mathbb{F}_{q^m})^n \longrightarrow (\mathbb{F}_{q^m})^n$ given by an invertible $n \times n$ matrix over $\mathbb{Z}/(q^m - 1)\mathbb{Z}$ that has exactly two nonzero entries in each row and each column; and such that the nonzero entries are all powers of p.
- An invertible linear map $L_3 : (\mathbb{F}_q)^{nm} \longrightarrow (\mathbb{F}_q)^{nm}$ given by a matrix that is the diagonal sum of n $m \times m$ boxes.

The following results can be checked by direct computations:

Lemma 2.1. *The maps G_1 and G_2 can be expressed as polynomial maps in $(\mathbb{F}_q)^{nm}$*

Lemma 2.2. *The composition of the five maps is a polynomial map in $(\mathbb{F}_q)^{nm}$, where each polynomial has at most $(m^2 \cdot (\lceil \frac{n}{m} \rceil + 1))^2$ monomials. Moreover, the variables and exponents that appear in each monomial depend only on the maps G_1 and G_2.*

Notice that the inverse maps G_1^{-1} and G_2^{-1} can be computed the same way from the inverse matrices and F^{-1} is also a polynomial. If the number of monomials in F^{-1} is not very big, one can get the coefficient of the polynomial by computing enough pairs $(x, F(x))$. To avoid this attack we take the exponent matrix of G_1, A_1 such that $d_1 = \frac{1}{\det(A_1)} \mod q^n - 1$ has an expansion in base p with many non-vanishing digits and the same for G_2.

The details of the construction can be found in the documentation presented to the NIST (see [7]). The parameters that we use and implement for the NIST proposal are $m = 3, n = 2$, $q = 2^{48}$ and the public key F has 6 polynomials with 64 monomials each and it has the remarkable property that each component of F^{-1} has at least 2^{100} monomials.

3. Security of the system DME

As in all multivariate systems, the way to invert the public key map F without the secret key is to solve the polynomial equations $F(x) = c$ (mainly) with a Gröbner basis algorithm. We have estimated the security against Gröbner basis attack and other standard attacks against multivariate systems (including some structural attacks). We performed many computer experiments using MAGMA and its implementation of the Faugere algorithm F4 with the public key polynomials DME for $q = 2^e$ and $2 < e < 9$. Our estimations are partial because F4 can find the Gröbner only up to $e = 5$ (30 bits). For $e = 6$ or higher F4 can not find the Gröbner basis because it exhausts the available RAM memory (512GB). The main experimental conclusion is that for those high degrees the complexity of computing the Gröbner basis is higher than an exhaustive search over all possible solutions. Another standard attack is to use the Weil descent, that is to represent F as a polynomial map Q over $\mathbb{F}_2$. Each of the monomials of F involves 4 variables with exponents 2^a. The polynomials in Q will have degree up to 4. There are no sharp estimates of the Gröbner basis complexity for quartic polynomials, this requires further research.

One promising attack to this kind of system is a structural one. For instance, we can set the entries of the matrices of L_1, L_2, L_3 as variables and compute the coefficients of the monomials. If we want to solve the resulting equations, we will get $6 \cdot 64$ equations in 48

variables of degree up to q. This might look like a hopeless task but, since the resulting coefficients are very structured, there might be specific techniques that could allow such an attack to work.

Regarding security against quantum computers, the only know attack is against quadratic systems ([4]).

References

[1] M. Avendaño, I. Luengo, M. Marco-Buzunariz On the security of the DME system. In preparation
[2] J. Ding, D. Schmidt, Solving degree and degree of regularity for polynomial systems over finite fields, Number theory and cryptography, pp. 34-49, Lecture Notes in Comput. Sci., 8260, Springer, Heidelberg, 2013.
[3] J. Ding, D. Schmidt, J. Gower. Multivariate Public Key Cryptography, Advances in Information Security series, Springer, 2006.
[4] JC. Faugère, K. Horan, D. Kahrobaei, M. Kaplan, E. Kashefi, and L. Perret. Fast quantum algorithm for solving multivariate quadratic equations. To appear. see https://eprint.iacr.org/2017/1236.pdf
[5] I. Luengo, Public key systems based on double exponentiation with matrix exponents, in preparation,.
[6] P. W. Shor, *Algorithms for quantum computation: Discrete logarithms and factoring*, in Proc. 35th Annual Symposium on Foundations of Computer Science, IEEE Computer Society Press, Los Alamitos, CA, pp. 124–134
[7] `https://www.mat.ucm.es/~iluengo/DME/`

Centro Universitario de la Defensa de Zaragoza
E-mail address: `avendano @ unizar.es`

Universidad Complutense de Madrid
E-mail address: `iluengo @ ucm.es`

Universidad de Zaragoza
E-mail address: `mmarco @ unizar.es`

Monografías de la Real Academia de Ciencias. Zaragoza. **43:** 51–53, (2018).
ISSN: 1132-6360

ON NORMAL SUBGROUP ZETA FUNCTIONS OF NILPOTENT GROUPS

TOMER BAUER

Abstract. For any natural number n, a finitely generated group G has only a finite number, say $a_n^{\triangleleft}$, of normal subgroups of index n. The normal subgroup zeta function of G is defined to be the Dirichlet series whose n-th coefficient is $a_n^{\triangleleft}$.

The aim of this talk is to be an introduction to the computation of normal subgroup zeta functions of torsion-free finitely generated nilpotent groups. Similar to the Riemann zeta function, these zeta functions have particularly nice properties. They have an Euler product decomposition to local factors indexed by primes, which are rational functions. Those local factors, in some cases, satisfy a functional equation. When possible, the use of a computer to explicitly compute the local factors and check for a functional equation, helps in motivating conjectures.

1. Introduction

Let G be a finitely generated group. For any natural number n, the group G has only a finite number of subgroups of index n. In their seminal paper, Gruneweld, Segal and Smith [1] start with this nice observation and use it to associate with G the Dirichlet series in the complex variable s,

$$\zeta_G(s) = \sum_{n=1}^{\infty} a_n n^{-s}$$

where a_n is the number of subgroups of G of index n. This series is *the subgroup zeta function of* G. The zeta function ζ_G can be seen as a non-commutative generalization of the Dedekind zeta function, which sums in a similar way the norm of the ideals in the ring of integers of a number field. The paper [1] and work by others have sprouted the research area of subgroup growth, as described in the manuscripts [2, 3] dedicated to the study of zeta functions of groups and rings.

While it is natural to count all subgroups (of finite index) in G, in the research area of subgroup growth a few other types of zeta functions are studied. The main object of this talk is one type already defined in [1]: the normal subgroup zeta function of the group G, defined to be

$$\zeta_G^{\triangleleft}(s) = \sum_{n=1}^{\infty} a_n^{\triangleleft} n^{-s}$$

where $a_n^{\triangleleft}$ is the number of normal subgroups of index n of G.

This talk will focus on computing normal subgroup zeta functions of torsion-free finitely generated nilpotent groups, or $\mathcal{T}$-groups for short. Computing explicit examples of the zeta functions is usually difficult, and we are able to do that in certain cases using the SageMath mathematics software system [4].

Let G be a $\mathcal{T}$-group. The function $\zeta_G^{\triangleleft}$ retains several of the nice properties of the Riemann zeta function, such as a decomposition into an Euler product of local factors:

$$\zeta_G^{\triangleleft}(s) = \prod_p \zeta_{G,p}^{\triangleleft}(s)$$

where the product is a formal product over all prime numbers and the factors

$$\zeta_{G,p}^{\triangleleft}(s) = \sum_{k=0}^{\infty} a_{p^k}^{\triangleleft} p^{-ks}$$

are the *local zeta functions* which enumerate only normal subgroups of G of p-power index. By [1, Theorem 1] these local factors are rational functions over $\mathbb{Z}$.

2. Higher Heisenberg groups over rings of integers

Definition 2.1. Let R be a commutative ring. For an integer $m \geq 1$ we define the *higher Heisenberg group of rank m over R* to be

$$H_m(R) = \left\{ \begin{pmatrix} 1 & \bar{a} & c \\ & I_m & \bar{b}^t \\ & & 1 \end{pmatrix} : \bar{a}, \bar{b} \in R^m, c \in R \right\} \subset SL_{m+2}(R)$$

where the matrix I_m is the $m \times m$ identity matrix.

For example $H_1(\mathbb{Z})$ is the well-known discrete Heisenberg group. In general, $H_m(R)$ is a centrally amalgamated direct product of m copies of the Heisenberg group over R. Let K be a number field and let $\mathcal{O}$ be its ring of integers. By sections 4 and 5 of [1] we can show a stronger form of the rationality of the local factors. There are a finite number of rational functions $W_1, \ldots, W_r$ of two variables over $\mathbb{Q}$ such that for any prime p, there exists $j \in \{1, \ldots, r\}$ such that $\zeta_{H_m(\mathcal{O}),p}^{\triangleleft} = W_j(p, p^{-s})$. The rational functions $W_1, \ldots, W_r$ only depend on the decomposition of the ideal $p\mathcal{O}$ in $\mathcal{O}$.

Grunewald, Segal and Smith [1] calculated the local factors $\zeta_{H_1(\mathcal{O}),p}^{\triangleleft}$ when K is a quadratic number field for any prime, and when K is a cubic number field for primes of some decomposition types. Results for $H_1(\mathcal{O})$ for arbitrary number fields were achieved by Schein and Voll [5, 6]. Their methods have many combinatorial aspects, and explicitly show the functional equation satisfied by a local factor. Using their methods and techniques allows us to calculate the local factors $\zeta_{H_m(\mathcal{O}),p}^{\triangleleft}$ for totally split primes in $\mathcal{O}$ and any m.

In many cases the local factors $\zeta_{G,p}^{\triangleleft}$ satisfy a functional equation upon inversion of the prime, of the form (cf. [3, Chapter 4]).

$$\zeta_{G,p}^{\triangleleft}(s)\big|_{p \to p^{-1}} = (-1)^c p^{b-as} \zeta_{G,p}^{\triangleleft}(s)$$

for some natural numbers c, a and b. We call $(-1)^c p^{b-as}$ the *symmetry factor* of the functional equation. Recall that a $\mathcal{T}$-group G has Hirsch length k if the maximal number of infinite cyclic factors G_i/G_{i-1} in any normal series $1 = G_0 \lhd G_1 \lhd \ldots \lhd G_n = G$ is k. Voll [7, Theorem C] proved that for any $\mathcal{T}$-group G of nilpotency class 2 (i.e. the derived

subgroup G' is abelian) of Hirsch length k such that $G/Z(G)$ has torsion-free rank d, for all but finitely many primes p,

$$\zeta^{\triangleleft}_{G,p}(s)\big|_{p\to p^{-1}} = (-1)^k p^{\binom{k}{2}-(d+k)s}\zeta^{\triangleleft}_{G,p}(s).$$

The higher Heisenberg groups $H_m(\mathcal{O})$ are of nilpotency class 2. Explicit computation in SageMath [4], as part of the author's M.Sc. thesis, of the local factors $\zeta^{\triangleleft}_{H_m(\mathcal{O}),p}$ for totally split primes used results such as the one above to test the correctness of the program. Examples computed in a computer algebra system can provide data in the study of the structure of the local factors. For non-split primes in $H_1(\mathcal{O})$, implementing a formula of Schein and Voll [6], we were able to check that the local factors are given in lowest terms (admit no cancellation) for number fields K of degree $[K:\mathbb{Q}] \leq 10$.

In another example, the local factor $\zeta^{\triangleleft}_{H_1(\mathcal{O}),p}$ for quartic fields and totally split p, was originally computed by Woodward and its numerator takes an entire page of the appendix of [3]. The methods of Schein and Voll [5] used a different method to compute it. The computer program implementing their method enables to quickly see that the two computations give the same result. Again, one can invert p and see that the symmetry factor match the expected theoretical results of Voll.

Acknowledgments. This work is partially supported by the Bar-Ilan University President's Doctoral Fellowships of Excellence Program. The author thank M. Schein and B. Greenfeld for valuable comments.

References

[1] F. J. Grunewald, D. Segal, and G. C. Smith, *Subgroups of finite index in nilpotent groups*, Invent. Math. **93** (1988), 185–223.

[2] A. Lubotzky and D. Segal. *Subgroup growth*, vol. **212** (2003) of *Progress in Mathematics*. Birkhäuser Verlag, Basel.

[3] M. P. F. du Sautoy and L. Woodward, *Zeta functions of groups and rings*, Lecture Notes in Mathematics, vol. **1925** (2008), Springer-Verlag, Berlin.

[4] The Sage Developers, *SageMath, the Sage Mathematics Software System* version 8.1 (2018), `http://www.sagemath.org`.

[5] M. M. Schein and C. Voll, *Normal zeta functions of the Heisenberg groups over number rings I – the unramified case*, J. Lond. Math. Soc. (2) **91** (2015), no. 1, 19–46.

[6] M. M. Schein and C. Voll, *Normal zeta functions of the Heisenberg groups over number rings II – the non-split case*, Israel J. Math. **211** (2016), 171–195.

[7] C. Voll, *Functional equations for zeta functions of groups and rings*, Ann. of Math. (2) **172** (2010), no. 2, 1181–1218.

Department of Mathematics, Bar-Ilan University, Ramat Gan 5290002, Israel

Monografías de la Real Academia de Ciencias. Zaragoza. **43:** 55–58, (2018).
ISSN: 1132-6360

CONSTRUCTION OF ALMOST REVLEX IDEALS WITH HILBERT FUNCTION OF SOME COMPLETE INTERSECTIONS

CRISTINA BERTONE AND FRANCESCA CIOFFI

Abstract. We give a constructive proof of the existence of the almost revlex ideal $J \subset K[x_1, \dots, x_n]$ with the same Hilbert function of a complete intersection generated by n forms of degrees $d_1 \leq \cdots \leq d_n$, when for every $i \geq 4$ the degrees $d_1, \dots, d_n$ satisfy the condition $d_i \geq \bar{u}_{i-1} + 1 = \min\Big\{ \Big\lfloor \frac{\sum_{j=1}^{i-1} d_j - i + 1}{2} \Big\rfloor, \sum_{j=1}^{i-2} d_j - i + 2 \Big\} + 1$.

Introduction

Let H be the Hilbert function of a complete intersection defined by n forms of degrees $d_1 \leq \cdots \leq d_n$ in n variables over a field K. We prove that if

$$(\star)\ \ d_i \geq \min\Big\{ \Big\lfloor \frac{\sum_{j=1}^{i-1} d_j - i + 1}{2} \Big\rfloor, \sum_{j=1}^{i-2} d_j - i + 2 \Big\} + 1,$$

for every $i \geq 4$, then there exists the almost revlex ideal J with Hilbert function H; further, every term of degree t outside J is divisible by the last variable, for every $t \geq \min\Big\{ \Big\lfloor \frac{\sum_{j=1}^{n} d_j - n}{2} \Big\rfloor, \sum_{j=1}^{n-1} d_j - n + 1 \Big\} + 1$.

The further property satisfied by J is crucial in our inductive and constructive proof of the above result, together with the combinatorial properties of the first expansion of the sous-escalier of a strongly stable ideal [9, 10] and the particular structure of the Hilbert function of a complete intersection [14]. Our proof follows a different approach from that used by Pardue in a more general case [13] and provides a new insight into the case of complete intersections generated by n generic forms.

According to Moreno-Socías' conjecture (see [11, Conjecture 4.1]), the almost revlex ideal J with the same Hilbert function of a complete intersection would be the generic initial ideal (with respect to degrevlex term order) of a polynomial ideal generated by generic forms. Indeed, the existence of J is interesting in the study of general schemes with a given Hilbert function in Algebraic Geometry.

To our knowledge, Moreno-Socías' conjecture has already been proved, mostly in characteristic 0, for $n = 2$ [1], for $n \leq 3$ [11, Proposition 4.2], for $n = 4$ and $d_1 = 2$ [8], if $d_i > (\sum_{j=1}^{i-1} d_j) - i + 1$ for every $i \geq 4$ [3, Corollary 2.12], if $d_i \geq (\sum_{j=1}^{i-1} d_j) - i - 1$ for every i [2, Theorem 3.19], and also in other particular cases [4]. It is noteworthy that Moreno-Socías' conjecture implies Fröberg's conjecture and Pardue's conjecture, which are equivalent to each other (see [7, 13, 3] and the references therein). For recent contributions to Fröberg's conjecture see [12, 6].

Date: May, 04 2018.

1. Background

Let $R := K[x_1, \dots, x_n]$ be the polynomial ring over an infinite field K in n variables endowed with the degree reverse lexicographic term order $\succ$ such that $x_1 \succ \cdots \succ x_n$. For every term $\tau := x_1^{\alpha_1} \dots x_n^{\alpha_n} \neq 1$, we let $\deg(\tau)$ be its degree and $\min(\tau) := \max\{i \mid \alpha_i \neq 0\}$. If $i = \min(\tau)$, we say that "τ has minimal variable x_i". Let $\mathbb{T}$ be the set of terms in R.

A subset $L \subset \mathbb{T}_t$ is a *revlex segment* if, for every $\tau \in L$ and $\tau' \in \mathbb{T}_t$, $\tau' \succ \tau$ implies that τ' belongs to L. A monomial ideal $J \subset R$ is a *revlex ideal* if $J_t \cap \mathbb{T}$ is a revlex segment, for every degree t, and is an *almost revlex ideal* if, for every minimal generator $\tau \in B_J$ of J, a term $\tau' \in \mathbb{T}_{\deg(\tau)}$ belongs to J if $\tau' \succ \tau$. A monomial ideal $J \subset R$ is *strongly stable* if for all $\tau \in J$ and for every variable x_i such that τ is divisible by x_i, the term $\frac{x_j \tau}{x_i}$ belongs to J, for every $x_j \succ x_i$. An almost revlex ideal is strongly stable. Letting $\mathcal{N}(J)$ be the set of terms outside J, we define the *first expansion* of $\mathcal{N}(J)_t$ as $\mathcal{E}(\mathcal{N}(J)_t) := \mathbb{T}_{t+1} \setminus (\{x_1, \dots, x_n\} \cdot J_t)$. $J_{\leq t}$ is the ideal generated by the terms of J of degree $\leq t$.

Remark 1.1. [9, 10] If $J \subset R$ is a strongly stable ideal, then for every degree t the first expansion $\mathcal{E}(\mathcal{N}(J)_t)$ of $\mathcal{N}(J)_t$ is equal to $\mathcal{N}(J_{\leq t})_{t+1}$ and can be directly computed without repetitions and in increasing order with respect to the reverse lexicographic order as follows:

$$\mathcal{E}(\mathcal{N}(J)_t) = x_n \cdot \mathcal{N}(J)_t \sqcup x_{n-1} \cdot \{\tau \in \mathcal{N}(J)_t : \min(\tau) \leq n-1\} \sqcup$$
$$\sqcup\, x_{n-2} \cdot \{\tau \in \mathcal{N}(J)_t : \min(\tau) \leq n-2\} \sqcup \cdots \sqcup x_1 \cdot \{\tau \in \mathcal{N}(J)_t : \min(\tau) \leq 1\}.$$

Thus, if ℓ is an integer such that $\mathcal{N}(J)_\ell \cap K[x_1, \dots, x_{n-1}] = \emptyset$ and H is the Hilbert function of R/J, then for all $t \geq \ell$ we have: $\mathcal{N}(J)_t \cap K[x_1, \dots, x_{n-1}] = \emptyset$ and $H(t) \geq H(t+1)$.

Notation 1.2. Let $d_1 \leq \cdots \leq d_n$ be n positive integers. For every $1 \leq i \leq n$, we set:
$m_i := (\sum_{j=1}^{i} d_j) - i$ and $\bar{u}_1 := 0$, $\bar{u}_i := \min\Big\{\lfloor \frac{m_i}{2} \rfloor, m_{i-1}\Big\}$.

From now, $I \subset R$ is the ideal generated by n generic forms of degrees $d_1 \leq \cdots \leq d_n$ and H the Hilbert function of R/I, $I' \subset K[x_1, \dots, x_{n-1}]$ is the ideal generated by $n-1$ generic forms of degrees $d_1 \leq \cdots \leq d_{n-1}$ and H' the Hilbert function of $K[x_1, \dots, x_{n-1}]/I'$. By standard methods of hypersurface sections, for every t we have $H(t) = \sum_{j=0}^{t} H'(j) - \sum_{j=0}^{t-d_n} H'(j)$.

Theorem 1.3. [5, 14] *The Hilbert function H is symmetric and the regularity of I is* $\operatorname{reg}(I) = \sum_{j=1}^{n} d_j - n + 1$. *Moreover, H is strictly increasing in the range $[0, \bar{u}_n]$ and is decreasing in the range $[\bar{u}_n, \operatorname{reg}(I)]$.*

Example 1.4. If $n = 4$ and $d_1 = 4$, $d_2 = 5$, $d_3 = 7$, $d_4 = 8$, then $m_1 = 3$, $m_2 = 7$, $m_3 = 13$, $m_4 = 20$, $\bar{u}_2 = 3$, $\bar{u}_3 = 6$, $\bar{u}_4 = 10$ and the Hilbert functions H and H' are:

t	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$H(t)$	1	4	10	20	34	51	70	89	105	116	120	116	105	89	70	…
$H'(t)$	1	3	6	10	14	17	19	19	17	14	10	6	3	1	0	…
$\Sigma_{j=0}^{t} H'(j)$	1	4	10	20	34	51	70	89	106	120	130	136	139	140	140	…

2. Main result and examples

We prove our main result by induction. First, we highlight parts of the inductive step.

Proposition 2.1. *Let $\bar{u}_n \geq t \geq d_n \geq \bar{u}_{n-1} + 1$ and $\widetilde{J} = \widetilde{J}_{\leq t} \subset R$ be an almost revlex ideal with $H_{R/\widetilde{J}}(h) = H(h)$, for every $h \leq t$, and $\mathcal{N}(\widetilde{J})_t$ consisting of*

$H(t-1)$ *terms with minimal variable* x_n,
$H'(t) - H'(t-d_n)$ *terms with minimal variable* x_{n-1}.

We can construct an almost revlex ideal $J = J_{\leq t+1}$ *with* $H_{R/J}(h) = H(h)$, $\forall\ h \leq t+1$ *and*

(1) *if* $\bar{u}_n > t$, *then* $\mathcal{N}(J)_{t+1}$ *consists of*
$H(t)$ *terms with minimal variable* x_n,
$H'(t+1) - H'(t+1-d_n)$ *terms with minimal variable* x_{n-1};
(2) *if* $\bar{u}_n = t$, *then* $\mathcal{N}(J)_{\bar{u}_n+1}$ *consists of terms with minimal variable* x_n.

Proposition 2.2. *Let* $t > \bar{u}_n$ *and* $\widetilde{J} = \widetilde{J}_{\leq t} \subset R$ *be almost revlex ideal with* $H_{R/\widetilde{J}}(h) = H(h)$, *for each* $h \leq t$, $\mathcal{N}(\widetilde{J})_t$ *made of terms with minimal variable* x_n. *We can construct the almost revlex ideal* J *so that* $H_{R/J} = H$ *and every term in* $\mathcal{N}(J)_v$ *is divisible by* x_n, *for every* $v \geq t$.

Theorem 2.3. (Main Result) *Assume* $d_i \geq \bar{u}_{i-1}+1$, *for every* $i \geq 4$. *Then, there exists the almost revlex ideal* $J \subset R$ *with Hilbert function* $H(t)$ *and every term in* $\mathcal{N}(J)_t$ *is divisible by* x_n, *for every* $t \geq \bar{u}_n + 1$.

Sketch of the Proof. We prove the statement by induction on n. If $n = 2$ the statement holds by [1, 11]. Assume $n \geq 3$. By the hypothesis, there exists the almost revlex ideal $\bar{J} \subset K[x_1, \ldots, x_{n-1}]$ with Hilbert function $H'(t)$ and all terms in $\mathcal{N}(\bar{J})_t$ divisible by x_{n-1}, for every $t \geq \bar{u}_{n-1}+1$. Consider the almost revlex ideal $\widetilde{J} := \bar{J}R \subset R$ with Hilbert function $H_{R/\widetilde{J}R}(t) = \sum_{j=0}^{t} H'(j)$. Starting from $\widetilde{J}$, we construct the almost revlex ideal J with Hilbert function $H(t)$ such that all terms in $\mathcal{N}(J)_t$ are divisible by x_n, for every $t \geq \bar{u}_n + 1$. We transform $\widetilde{J}$ by removing suitable terms from the sous-escalier of $\widetilde{J}$ at every degree $t \geq d_n$, in order to decrease its Hilbert function, which is greater than $H(t)$. The properties of the Hilbert function of a complete intersection that are collected in the statement of Theorem 1.3 guarantee that the first expansion of $\mathcal{N}(\widetilde{J})_t$, for every $t \geq d_n$, is enough big to remove the greatest possible terms and obtain the desired almost revlex ideal J.

First, we consider the case $\bar{u}_n \geq d_n \geq \bar{u}_{n-1} + 1$ and begin our construction by setting $J_t = \widetilde{J}_t$, for each $t < d_n$, and observing that $H(d_n) = \sum_{j=0}^{d_n} H'(j) - H'(0)$. Hence, at degree $t = d_n$ we need to remove only $1 = H'(0)$ term from $\mathcal{N}(\widetilde{J})_{d_n}$. From the hypothesis we have $d_n \leq \bar{u}_n \leq m_{n-1}$. Then, we can choose the highest possible term τ in $\mathcal{N}(\widetilde{J})_{d_n}$ divisible by x_{n-1}, because $H'(d_n) \neq 0$. So, we define $J_{d_n} := \langle \widetilde{J}_{d_n} \cup \{\tau\} \rangle$ and obtain $\mathcal{N}(J)_{d_n}$ made of
$H(d_n - 1)$ terms with minimal variable x_n,
$H'(d_n) - H'(0)$ terms with minimal variable x_{n-1}.
Now, we can assume to have $J_{\leq t}$ satisfying the hypotheses of Proposition 2.1 and apply Proposition 2.1 up to the degree $\bar{u}_n + 1$, in order to obtain the condition that every term of degree $\bar{u}_n + 1$ outside J is divisible by x_n. Then, we can apply Proposition 2.2. The conditions listed in Remark 1.1 and Theorem 1.3 guarantee that the construction of J can go on until the regularity of J. The other cases analogously follow. □

Example 2.4. Consider the Hilbert function H : 1 3 6 9 10 9 6 3 1 of a complete intersection generated by 3 forms of degrees $d_1 = 3$, $d_2 = 4$, $d_3 = 4$ in $K[x_1, x_2, x_3]$. We have $\bar{u}_2 = 2$ and $\bar{u}_3 = 4$ and there exists the almost revlex ideal $J \subset K[x_1, x_2, x_3]$ with Hilbert function H: $J = (x_1^3, x_2^2x_1^2, x_2^3x_1, x_2^5, x_3x_2^4, x_3^3x_2x_1^2, x_3^3x_2^2x_1, x_3^3x_2^3, x_3^5x_1^2, x_3^5x_2x_1, x_3^5x_2^2, x_3^7x_1, x_3^7x_2, x_3^9)$. We can see that the term x_2^4 belongs to $\mathcal{N}(J)_4$. Hence, there is a term of degree $\bar{u}_3 = 4$ outside

J which is not divisible by the last variable x_3. Thus, the result of Theorem 2.3 concerning the divisibility of the terms in $\mathcal{N}(J)$ by the last variable is sharp.

Example 2.5. Theorem 2.3 can be applied to the cases that have been considered in Examples 1.4 and 2.4 and also if $n = 4$, $d_1 = 3$, $d_2 = 4$, $d_3 = 4$, $d_4 = 8$, so we have $\bar{u}_2 = 3$, $\bar{u}_3 = 4$, $\bar{u}_4 = 7$ and $d_4 = \bar{u}_4 + 1 \geq \bar{u}_3 + 1$. The Hilbert functions are:

t	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$H(t)$	1	4	10	19	29	38	44	47	47	44	38	29	19	10	4	1
$H'(t)$	1	3	6	9	10	9	6	3	1	0	0	0	0	0	...	
$\Sigma_{j=0}^{t} H'(j)$	1	4	10	19	29	38	44	47	48	48	48	48	48	48	...	

References

[1] Edith Aguirre, Abdul Salam Jarrah, and Reinhard Laubenbacher, *Generic ideals and Moreno-Socías conjecture*, Proceedings of the 2001 International Symposium on Symbolic and Algebraic Computation, ACM, New York, 2001, pp. 21–23.

[2] Juliane Capaverde and Shuhong Gao, *Gröbner Bases of Generic Ideals*, Available at http://arxiv.org/abs/1711.05309, 2017, Preprint.

[3] Young Hyun Cho and Jung Pil Park, *Conditions for generic initial ideals to be almost reverse lexicographic*, J. Algebra **319** (2008), no. 7, 2761–2771. MR 2397406

[4] Mircea Cimpoeaş, *A note on the generic initial ideal for complete intersections*, Bull. Math. Soc. Sci. Math. Roumanie (N.S.) **50(98)** (2007), no. 2, 119–130.

[5] E. D. Davis, A. V. Geramita, and F. Orecchia, *Gorenstein algebras and the Cayley-Bacharach theorem*, Proc. Amer. Math. Soc. **93** (1985), no. 4, 593–597. MR 776185

[6] Duc Trung Van, *Fröberg's Conjecture and the initial ideal of generic sequences*, Available at https://arxiv.org/abs/1803.04997, 2018, Preprint.

[7] Ralf Fröberg, *An inequality for Hilbert series of graded algebras*, Math. Scand. **56** (1985), no. 2, 117–144.

[8] Tadahito Harima, Sho Sakaki, and Akihito Wachi, *Generic initial ideals of some monomial complete intersections in four variables*, Arch. Math. (Basel) **94** (2010), no. 2, 129–137. MR 2592759

[9] F. S. Macaulay, *Some properties of enumeration in the theory of modular systems*, Proc. London Math. Soc. (1926), no. 26, 531–555.

[10] Maria Grazia Marinari and Luciana Ramella, *Some properties of Borel ideals*, J. Pure Appl. Algebra **139** (1999), no. 1-3, 183–200, Effective methods in algebraic geometry (Saint-Malo, 1998).

[11] Guillermo Moreno-Socías, *Degrevlex Gröbner bases of generic complete intersections*, J. Pure Appl. Algebra **180** (2003), no. 3, 263–283.

[12] Gleb Nenashev, *A note on Fröberg's conjecture for forms of equal degrees*, C. R. Math. Acad. Sci. Paris **355** (2017), no. 3, 272–276.

[13] Keith Pardue, *Generic sequences of polynomials*, J. Algebra **324** (2010), no. 4, 579–590.

[14] Les Reid, Leslie G. Roberts, and Moshe Roitman, *On complete intersections and their Hilbert functions*, Canad. Math. Bull. **34** (1991), no. 4, 525–535.

Dipartimento di Matematica "G. Peano", University of Turin, Italy
E-mail address: cristina.bertone@unito.it

Dip. di Matematica e Appl. "R. Caccioppoli", University of Naples Federico II, Italy
E-mail address: cioffifr@unina.it

Monografías de la Real Academia de Ciencias. Zaragoza. **43:** 59–62, (2018).
ISSN: 1132-6360

TWO NEW CHARACTERIZATIONS OF FREE HYPERPLANE ARRANGEMENTS

ANNA MARIA BIGATTI, ELISA PALEZZATO, AND MICHELE TORIELLI

Abstract. We describe two new characterizations of freeness for hyperplane arrangements via the study of the generic initial ideal and of the sectional matrix of the Jacobian ideal of arrangements. Moreover, we will show the new package `arrangements` fot the software CoCoA.

1. Introduction

An arrangement of hyperplanes is a finite collection of codimension one affine subspaces in a finite dimensional vector space. Associated to these spaces, there is a plethora of algebraic, combinatorial and topological invariants. Arrangements are easily defined but they lead to deep and beautiful results that put in connection various area of mathematics. We refer to [9] for a comprehensive treatment of the subject.

In the theory of hyperplane arrangements, the freeness of an arrangement is a key notion which connects arrangement theory with algebraic geometry and combinatorics. The notion of freeness was introduced by Saito in [11] for the case of hypersurfaces in the analytic category. The special case of hyperplane arrangements was firstly studied by Terao in [12], where he showed that we can pass from analytic to algebraic considerations. By definition, an arrangement is free if and only if its module of logarithmic derivations is a free module. It turns out that, by Terao's characterization [9], this notion is equivalent to the requirement that the Jacobian ideal of the arrangement (the ideal generated by the defining equation and its partial derivatives) is Cohen-Macaulay of codimension 2. To check freeness for a given arrangement, or to construct new free arrangements, is a very difficult task though it is very fundamental.

We will give new characterizations of freeness for any dimension. Namely, starting from the result of Terao, we characterize freeness in terms of the generic initial ideal and of the sectional matrix of the Jacobian ideal $J(\mathcal{A})$ of the arrangement $\mathcal{A}$, Moreover, we will describe the package `arrangements` that we developed for the software CoCoA.

These results are part of [5] and [10].

2. Preliminares on hyperplane arrangements

Let K be a field of characteristic zero. A finite set of affine hyperplanes $\mathcal{A} = \{H_1, \dots, H_n\}$ in K^l is called a **hyperplane arrangement**. For each hyperplane H_i we fix a defining equation $\alpha_i \in S = K[x_1, \dots, x_l]$ such that $H_i = \alpha_i^{-1}(0)$, and let $Q(\mathcal{A}) = \prod_{i=1}^n \alpha_i$. An arrangement $\mathcal{A}$ is called **central** if each H_i contains the origin of K^l.

We denote by $\mathrm{Der}_{K^l} = \{\sum_{i=1}^l f_i \partial_{x_i} \mid f_i \in S\}$ the S-module of **polynomial vector fields** on K^l (or S-derivations). Let $\delta = \sum_{i=1}^l f_i \partial_{x_i} \in \mathrm{Der}_{K^l}$. Then δ is said to be **homogeneous of polynomial degree** d if $f_1, \dots, f_l$ are homogeneous polynomials of degree d in S. In this case, we write $\mathrm{pdeg}(\delta) = d$.

A central arrangement $\mathcal{A}$ is said to be **free with exponents** $(e_1, \dots, e_l)$ if and only if the module of vector fields logarithmic tangent to $\mathcal{A}$, $D(\mathcal{A}) = \{\delta \in \mathrm{Der}_{K^l} \mid \delta(\alpha_i) \in \langle \alpha_i \rangle S, \forall i\}$, is a free S-module and there exists a basis $\delta_1, \dots, \delta_l \in D(\mathcal{A})$ such that $\mathrm{pdeg}(\delta_i) = e_i$, or equivalently $D(\mathcal{A}) \cong \bigoplus_{i=1}^{l} S(-e_i)$.

3. New characterizations of free hyperplane arrangements

We firstly characterize freeness by looking at the generic initial ideal $\mathrm{rgin}(J(\mathcal{A}))$ of the Jacobian ideal $J(\mathcal{A})$ of $\mathcal{A}$ with respect to the term ordering degrevlex. In this setting, the generic initial ideal of a polynomial ideal I with respect to a term ordering σ is the unique monomial ideal J such that $J = \mathrm{LT}_\sigma(g(I))$, where g is a generic change of coordinates. For the detailed definition and the basic properties of generic initial ideals, we refer to [7] and [8].

Theorem 3.1. *Let $\mathcal{A} = \{H_1, \dots, H_n\}$ be a central arrangement in K^l. Then $\mathcal{A}$ is free if and only if* $\mathrm{rgin}(J(\mathcal{A}))$ *is S or its minimal generators include x_1^{n-1}, some positive power of x_2, and no monomials in $x_3, \dots, x_l$. More precisely, if $\mathcal{A}$ is free, then* $\mathrm{rgin}(J(\mathcal{A}))$ *is S or it is minimally generated by*

$$x_1^{n-1},\ x_1^{n-2}x_2^{\lambda_1},\ \dots,\ x_2^{\lambda_{n-1}}$$

with $1 \le \lambda_1 < \lambda_2 < \cdots < \lambda_{n-1}$ and $\lambda_{i+1} - \lambda_i = 1$ or 2.

In the example at the end of the next section, we can see that the generic initial ideal of the Jacobian ideal of the Braid arrangement involves only the first two variables, in fact the Braid arrangement is free.

If we look at the resolution of the $\mathrm{rgin}(J(\mathcal{A}))$, we can not only see if $\mathcal{A}$ is free but also compute its exponents.

Theorem 3.2. *Let $\mathcal{A} = \{H_1, \dots, H_n\}$ be an essential and central arrangement in K^l, with $l \ge 2$. If $\mathcal{A}$ is free with exponents $(e_1, \dots, e_l)$ then* $\mathrm{rgin}(J(\mathcal{A}))$ *has free resolution*

$$0 \longrightarrow \bigoplus_{j=n-1}^{n+e_l-2} S(-j-1)^{\beta_{1,j+1}} \longrightarrow \bigoplus_{j=n-1}^{n+e_l-2} S(-j)^{\beta_{0,j}} \longrightarrow \mathrm{rgin}(J(\mathcal{A})) \longrightarrow 0,$$

where $\beta_{0,n-1} = \beta_{1,n}+1 = l$ and $\beta_{1,j+1} = \beta_{0,j} = \#\{i \mid e_i > j-n+1\}$ for all $j \ge n$. In particular, $\beta_{0,n-1} > \beta_{0,n} \ge \cdots \ge \beta_{0,n+e_l-2}$.

We now characterize freeness by looking at the sectional matrix of $S/J(\mathcal{A})$. In this setting, the sectional matrix $\mathcal{M}_{S/I}$ of a polynomial ideal I encodes the Hilbert functions of successive hyperplane sections of the quotient S/I. In particular, $\mathcal{M}_{S/I}(i, -)$ is the Hilbert function of the quotient $S/(I + (L_1, \dots, L_{l-i}))$, where L_k are generic linear forms. For the detailed definition and basic properties of sectional matrices, we refer to [6] and [4].

Theorem 3.3. *Let $\mathcal{A}$ be a central arrangement and $d_0 = \max\{d \mid \mathcal{M}_{S/J(\mathcal{A})}(2, d) \neq 0\}$. Then $\mathcal{A}$ is free if and only if $\mathcal{M}_{S/J(\mathcal{A})}$ is the zero function or the following two conditions hold*

(1) $\mathcal{M}_{S/J(\mathcal{A})}(3, d_0) = \mathcal{M}_{S/J(\mathcal{A})}(3, d_0+1) = \mathcal{M}_{S/J(\mathcal{A})}(3, d_0+2)$,
(2) $\mathcal{M}_{S/J(\mathcal{A})}(3, d_0) = \sum_{d=0}^{d_0} \mathcal{M}_{S/J(\mathcal{A})}(2, d)$.

In the example at the end of the next section, we can see that the sectional matrix of the Jacobian ideal of the Braid arrangement satisfies both the conditions of the previous theorem.

With the notation of the previous theorem, d_0 coincides with $\min\{d \mid x_2^{d+1} \in \operatorname{rgin}(J(\mathcal{A}))\}$.

Conjecture 3.4. *Let $\mathcal{A} = \{H_1, \ldots, H_n\}$ be a central arrangement in K^l. If $\operatorname{rgin}(J(\mathcal{A}))$ has a minimal generator T that involves the third variable of S, then $\deg(T) \geq d_0 + 1$.*

If the previous conjecture is true, then the statement of Theorem 3.3 becomes easier, as follows:

Corollary 3.5. *Let $\mathcal{A}$ be a central arrangement. Then $\mathcal{A}$ is free if and only if $\mathcal{M}_{S/J(\mathcal{A})}$ is the zero function or $\mathcal{M}_{S/J(\mathcal{A})}(3, d_0) = \mathcal{M}_{S/J(\mathcal{A})}(3, d_0{+}1) = \mathcal{M}_{S/J(\mathcal{A})}(3, d_0 + 2)$.*

4. Arrangement package for CoCoA

In order to test our theorems and play with examples, the second and third authors (see [10]) wrote the package `arrangements` for the software CoCoA, see [1], [2] and [3]. This package will be part of the official release CoCoA-5.2.4.

This package allows the user to easily define any hyperplane arrangement. Moreover, several known families of arrangements are already implemented. For example, we can construct the Braid arrangement in CoCoA as follows:

```
/**/ use S::=QQ[x,y,z];
/**/ A := ArrBraid(S,3);A;
[x-y,  x-z,  y-z]
```

With this package, we can compute several combinatorial invariants of hyperplane arrangements. For example, we can construct the flats of the intersection lattice, the characteristic and the Tutte polynomials, and the Betti numbers of the Braid arrangement in CoCoA as follows:

```
/**/ ArrFlats(A);
[[ideal(0)], [ideal(x-y), ideal(x-z), ideal(y-z)], [ideal(x-z,y-z)]]
/**/ ArrCharPoly(A);
t^3-3*t^2+2*t
/**/ ArrTuttePoly(A);
t[1]^2+t[1]+t[2]
/**/ ArrBettiNumbers(A);
[1,  3,  2]
```

We can also compute various algebraic invariants. For example, we can construct the Orlik-Terao ideal of the Braid arrangement in CoCoA as follows:

```
/**/ OrlikTeraoIdeal(A);
ideal(y[1]*y[2]-y[1]*y[3]+y[2]*y[3])
```

Moreover, several functions for the class of free hyperplane arrangements are implemented. In addition, this package allows also to do computations with multiarrangements. We can check freeness, compute a Saito's matrix, the exponents, the generic initial ideal and the sectional matrix of the Braid arrangement in CoCoA as follows:

```
/**/ IsArrFree(A);
true
```

```
/**/ ArrDerMod(A);
matrix( /*RingWithID(3, "QQ[x,y,z]")*/
 [[1, 0, 0],
  [1, x-y, 0],
  [1, x-z, x*y-x*z-y*z+z^2]])
/**/ ArrExponents(A);
[0,  1,  2]
/**/ Q:=product(A);
/**/ GinJacobian(Q);
ideal(x^2,  x*y,  y^3)
/**/ PrintSectionalMatrix(S/ideal(GensJacobian(Q)));
  0  1  2  3  4
  -  -  -  -  -
  1  1  0  0  0
  1  2  1  0  0
  1  3  4  4  4
```

References

[1] J. Abbott and A.M. Bigatti. CoCoALib: a C++ library for doing Computations in Commutative Algebra. Available at `http://cocoa.dima.unige.it/cocoalib`, 2016.

[2] J. Abbott and A.M. Bigatti. Gröbner bases for everyone with CoCoA-5 and CoCoALib. *Advanced Studies in Pure Mathematics*, 77:1–24, 2018.

[3] J. Abbott, A.M. Bigatti, and L. Robbiano. CoCoA: a system for doing Computations in Commutative Algebra. Available at `http://cocoa.dima.unige.it`.

[4] A. Bigatti, E. Palezzato, and M. Torielli. Extremal behavior in sectional matrices. *Journal of Algebra and its Applications*, https://doi.org/10.1142/S0219498819500415, 2018.

[5] A. Bigatti, E. Palezzato, and M. Torielli. New characterizations of freeness for hyperplane arrangements. *arXiv:1801.09868*, 2018.

[6] A. Bigatti and L. Robbiano. Borel sets and sectional matrices. *Annals of Combinatorics*, 1(1):197–213, 1997.

[7] A. Galligo. A propos du théoreme de préparation de Weierstrass. In *Fonctions de plusieurs variables complexes*, pages 543–579. Springer, 1974.

[8] J. Herzog and T. Hibi. *Monomial ideals*. Springer, 2011.

[9] P. Orlik and H. Terao. *Arrangements of hyperplanes*, volume 300 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1992.

[10] E. Palezzato and M. Torielli. Hyperplane arrangements in CoCoA. *arXiv preprint arXiv:1805.02366*, 2018.

[11] K. Saito. Theory of logarithmic differential forms and logarithmic vector fields. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 27(2):265–291, 1980.

[12] H. Terao. Arrangements of hyperplanes and their freeness I. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 27(2):293–312, 1980.

University of Genova, Department of Mathematics
E-mail address: `bigatti@dima.unige.it`

Hokkaido University, Department of Mathematics
E-mail address: `palezzato@math.sci.hokudai.ac.jp`

Hokkaido University, Department of Mathematics
E-mail address: `torielli@math.sci.hokudai.ac.jp`

Monografías de la Real Academia de Ciencias. Zaragoza. **43:** 63–65, (2018).
ISSN: 1132-6360

EQUATIONS FOR THE FLEX LOCUS OF A HYPERSURFACE

LAURENT BUSÉ, CARLOS D'ANDREA, MARTÍN SOMBRA, AND MARTIN WEIMANN

Abstract. For a degree d surface in projective space with no ruled components, a theorem of Salmon asserts that the flex locus is a curve on this surface of degree at most $11d^2 - 24d$. We generalise this result to hypersurfaces of arbitrary dimension and compute explicit equations of the flex locus by using multidimensional resultant theory. For generic hypersurfaces, we show that our degree bound is reached and that the generic flex line is unique and with expected contact order.

The flex locus of a projective hypersurface is the subset of points through which there is a line with higher contact order than expected. For a plane projective curve, the flex locus is well known: it is the set of inflexion points and it is given by the intersection of the curve with the zero locus of the Hessian. In this article, we study the basic geometry of the flex locus. In particular, we address the problem of computing the dimension, degree and equations of the flex locus of a hypersurface of a projective space of arbitrary dimension.

Let $\mathbb{K}$ be an algebraically closed field of characteristic zero and $V \subset \mathbb{P}^n$ a subvariety of the n-dimensional projective space over $\mathbb{K}$. The *osculating order* of V at a point $p \in \mathbb{P}^n$ is the maximum contact order at p between V and a line. We denote it by $\mu_p(V)$. An irreducible variety is ruled if it is a union of lines or, equivalently, if the osculating order is infinite for all points $p \in V$. In addition, we say that a property holds for a *generic* element in a family if it holds outside a proper Zariski closed subset of this family.

The following result is a consequence of [Lan99, Generic Theorem]:

Theorem 0.1. *Let $V \subset \mathbb{P}^n$ be a hypersurface with no ruled components, and $p \in V$. Then $\mu_p(V) \geq n$ and the equality holds for a generic $p \in V$.*

This result leads to the following definition:

Definition 0.2. We call the *flex locus* of a projective hypersurface $V \subset \mathbb{P}^n$ the subset

$$\mathrm{Flex}(V) = \{p \in V \mid \mu_p(V) > n\}.$$

A point $p \in \mathrm{Flex}(V)$ is called a *flex point*. A line with contact order larger than n at some point of V is called a *flex line*.

Let us first summarize the known results in the case of curves and surfaces.

Theorem 0.3. *Let $C \subset \mathbb{P}^2$ be a plane curve of degree d which does not contain any line. Then C contains at most $3d^2 - 6d$ flex points.*

This result follows directly from the fact that $p \in C$ is a flex point if and only if the Hessian of the homogeneous polynomial equation of C vanishes at p (see for instance [BK86,

Thm.1, Ch.7.3]). In the case of surfaces, the following result is due to Salmon [Sal49, Ch.VI] but it has been revisited by several authors since then (e.g. [Kat14, EH13]):

Theorem 0.4. *Let $S \subset \mathbb{P}^3$ be a surface of degree d with no ruled components. Then Flex(S) is a curve on S of degree at most $11d^2 - 24d$.*

In particular, if $d = 3$, we get that $\deg \mathrm{Flex}(S) \leq 27$. Since a flex line of a cubic surface S has contact order ≥ 4, it is necessarily contained in S by Bezout's theorem: we recover the classical fact that a cubic contains at most 27 lines (and it turns out to be the exact number when S is smooth).

Our first main theorem generalises these results to hypersurfaces of arbitrary dimension. Its proof follows the original proof given by Salmon in the case of surfaces and leads to the construction of explicit equations for the flex locus. To be more precise, let us introduce two sets of variables

$$x = (x_0, \ldots, x_n) \quad \text{and} \quad y = (y_0, \ldots, y_n).$$

To any homogeneous polynomial $F \in \mathbb{K}[x]$, we associate the family of homogeneous polynomials $F_0, \ldots, F_d \in \mathbb{K}[x, y]$ which are uniquely determined by the formula

$$F(x + ty) = \sum_{k=0}^{d} F_k(x, y) \frac{t^k}{k!}. \tag{1}$$

For all $k = 0, \ldots, d$, the polynomial F_k is bihomogeneous of bidegree $(d-k, k)$ with respect to x and y and it admits an explicit expression that depends on the k^{th}-order partial derivatives of F. In particular, we have that $F_0(x, y) = F(x)$ and $F_d(x, y) = F(y)$. Below, the resultant operator of $n + 1$ homogeneous polynomials in the $n + 1$ variables $y_0, \ldots, y_n$ is denoted by $\mathrm{Res}_y(\cdot)$.

Theorem 0.5. *Let $V \subset \mathbb{P}^n$ be a hypersurface defined by a square-free polynomial F of degree d. If $d < n$, all components of V are ruled. If $d \geq n$, then either V has a ruled component or Flex(V) is a codimension 1 subvariety of V with equations*

$$\mathit{Flex}(V) = \{F = P = 0\}, \tag{2}$$

where $P \mod F$ is uniquely determined by

$$\mathit{Res}_y(F_1, \ldots, F_n, y_0) \equiv x_0^{n!} P \mod F. \tag{3}$$

Moreover, in this case the flex locus is equipped with a scheme structure and we have that

$$\deg \mathit{Flex}(V) = d^2 \sum_{k=1}^{n} \frac{n!}{k} - d(n+1)! \tag{4}$$

Example 0.6. Let $C = \{F = 0\} \subset \mathbb{P}^2$ be a smooth curve of degree d. A straightforward computation using the Euler identities shows that

$$-(d-1)^2 \mathrm{Res}_y(F_1, F_2, y_0) \equiv x_0^2 \det(H_F) \mod F, \tag{5}$$

where H_F stands for the Hessian of F (determinant of the Hessian matrix): we recover the well–known fact that $p \in C$ is a flex if and only if the Hessian of F vanishes at p.

Our second main result ensures that the degree bound is sharp and that the expected properties of the flex locus hold in the generic case. More precisely :

Theorem 0.7. *For F a generic polynomial of degree $d \geq n$, the subscheme $Z(F, P)$ defined by (2) and (3) is reduced and the degree bound (4) is reached. Moreover, through a generic flex point, there is a unique flex line, and this line has contact order exactly $n + 1$ (or is contained in V if $d = n$).*

We conclude by mentioning that giving a closed form for a canonical representative for P modulo F in Theorem 0.5 seems to be a challenge on its own. In the case of curves, such a representative is given by the Hessian. For $n = 3$, Salmon also obtained a representative of this polynomial as a determinantal closed formula in terms of covariants, based on an approach by Clebsch [Sal65, Articles 589 to 597]. It would be interesting to generalize these formulae to higher dimensions.

Acknowledgements. All authors where supported by the CNRS PICS 6381 "Géométrie diophantienne et calcul formel". D'Andrea and Sombra also acknowledge financial support from the Spanish MINECO, through the research project MTM2015-65361-P, and the "María de Maeztu" Programme for Units of Excellence in R&D (MDM-2014-0445).

References

[BK86] E. Brieskorn, H. Knörrer, *Plane algebraic curves*, Birkhäuser Basel, 1986.

[EH13] D. Eisenbud, J. Harris. *3264 and All That; Intersection Theory in Algebraic Geometry.* Cambridge University Press; 1 edition, 2016.

[Kat14] N. Katz. *The flecnode polynomial: a central object in incidence geometry.* Proceedings of the 2014 ICM, arXiv:1404:3412.

[Lan99] J. M. Landsberg. *Is a linear space contained in a submanifold? – On the number of derivatives needed to tell.* J. Reine Angew. Math. 508 (1999), 53–60.

[Sal49] G. Salmon. *On the triple tangent planes to a surface of the third order,* Cambridge and Dublin Math. Journal 4 (1849), 252–260.

Université Côte d'Azur, Inria, 2004 route des Lucioles, 06902 Sophia Antipolis, France
E-mail address: Laurent.Buse@inria.fr
URL: http://www-sop.inria.fr/members/Laurent.Buse/

Departament de Matemàtiques i Informàtica, Universitat de Barcelona. Gran Via 585, 08007 Barcelona Spain
E-mail address: cdandrea@ub.edu
URL: http://www.ub.edu/arcades/cdandrea.html

ICREA. Passeig Lluís Companys 23, 08010 Barcelona, Spain & Departament de Matemàtiques i Informàtica, Universitat de Barcelona. Gran Via 585, 08007 Barcelona Spain
E-mail address: sombra@ub.edu
URL: http://www.maia.ub.es/~sombra

Université de Caen UMR CNRS 6139 BP 5186 -14032 Caen Cedex, France & GAATI (University of French Polynesia), BP 6570 - 98702 Faaa
E-mail address: weimann@unicaen.fr
URL: https://weimann.users.lmno.cnrs.fr/

Monografías de la Real Academia de Ciencias. Zaragoza. **43:** 67–70, (2018).
ISSN: 1132-6360

ON THE b-FUNCTION OF HYPERGEOMETRIC IDEALS ASSOCIATED WITH SOME SPACE CURVES

F.-J. CASTRO-JIMÉNEZ AND H. COBO PABLOS

Abstract. In this paper we study the b-function with respect to a weight vector, associated to a hypergeometric ideal $H_A(\beta)$, with A of the form $(1, p, q)$ and β any complex number.

Introduction

The Bernstein polynomial, also called Bernstein-Sato polynomial, associated with a given nonzero polynomial $f \in \mathbb{C}[x]$ has been introduced by J. Bernstein in [3] and independently by M. Sato in [20]. We denote by $D_n := \mathbb{C}[x_1, \ldots, x_n, \partial_1, \ldots, \partial_n]$ the Weyl algebra over the field $\mathbb{C}$ and $D_n[s] := D_n \otimes_{\mathbb{C}} \mathbb{C}[s]$ where s is a new indeterminate.

Theorem 0.1. [3] *Let $f \in \mathbb{C}[x]$ be nonzero. There exists a nonzero polynomial $b(s) \in \mathbb{C}[s]$ and a differential operator $P(s) \in D_n[s]$ such that*

$$P(s)f(f^s) = b(s)f^s.$$

The set of polynomials $b(s)$ satisfying the equation in Theorem 0.1 for some $P(s) \in D_n[s]$ is a nonzero ideal in $\mathbb{C}[s]$. Its unique monic generator is denoted by $b_f(s)$.

Definition 0.2. The polynomial $b_f(s)$ is called the Bernstein, or the Bernstein-Sato, polynomial associated with f.

A fundamental result in singularity theory assures that the roots of $b_f(s)$ are negative rational numbers [12], [9]. There are several algorithms for computing Bernstein polynomials: see [16], [17], [15], [8], [14], [6], [7], [1] and the references therein. Nevertheless, $b_f(s)$ is hard to compute even in the case of a polynomial f in two variables [23], [2]. In [11] the authors propose the algorithm `checkRoot` which, given a rational number α checks if it is a root of the Bernstein polynomial $b_f(s)$, and computes its multiplicity.

More generally, given a holonomic left ideal I in D_n and a nonzero weight vector $\omega \in \mathbb{R}^n$, M. Kashiwara has introduced in [10, §2] the b–function $b_{I,\omega}(s)$ associated with the pair (I, ω), as the monic generator of the ideal

$$in_{(-\omega,\omega)}(I) \cap \mathbb{C}[s] \tag{1}$$

where $s := \sum_{i=1}^n \omega_i x_i \partial_i$, and $in_{(-\omega,\omega)}(I)$ is the initial ideal of $I \subset D_n$ with respect to the filtration induced on D_n by the vector $(-\omega, \omega) \in \mathbb{R}^{2n}$, that is the filtration given by the vector spaces

$$F_p = \mathbb{C}\{x^\alpha \partial^\beta \mid -\omega\alpha + \omega\beta \leq p\} \quad \text{for } p \in \mathbb{R}.$$

It is proven in [10, Theorem 2.7] that the ideal in (1) is nonzero. We are following here the presentation and notations of [22, §5] of this subject.

Definition 0.3. The polynomial $b_{I,\omega}(s)$ is called the b–function of the holonomic ideal $I \subset D_n$ with respect to the weight vector ω.

Both notions, Bernstein polynomial and b–function are closely related: the first one $b_f(s)$ equals $b_{I,\omega}(-s-1)$ by considering $I \subset D_{n+1} = \mathbb{C}[x_1, \ldots, x_n, x_{n+1}, \partial_1, \ldots, \partial_n, \partial_{n+1}]$ as the ideal generated by the set

$$\{x_{n+1} - f(x), \partial_1 + \frac{\partial f}{\partial x_1}\partial_{n+1}, \ldots, \partial_n + \frac{\partial f}{\partial x_n}\partial_{n+1}\}$$

and $\omega = (0, \ldots, 0, 1) \in \mathbb{R}^{n+1}$, see e.g. [22, Lema 5.3.11].

1. b-function of hypergeometric ideals

Here we study the b–function associated with some hypergeometric ideals $H_A(\beta) \subseteq D_n$ following [22, Section 5.1]. Let us recall the definition of $H_A(\beta)$. Given $A = (a_{ij})$ a $d \times n$ matrix of rank d with integer coefficients we define the associated toric ideal

$$I_A := \mathbb{C}[\partial]\{\partial^u - \partial^v \mid u, v \in \mathbb{N}^n, Au = Av\}.$$

For any parameter vector $\beta \in \mathbb{C}^d$ and for $1 \leq i \leq d$, we consider the Euler operators $E_i - \beta_i := a_{i1}x_1\partial_1 + \cdots + a_{in}x_n\partial_n - \beta_i$. The hypergeometric ideal is defined as

$$H_A(\beta) := D_n \cdot I_A + \sum_{1 \leq i \leq d} D_n(E_i - \beta_i).$$

More specifically, in this paper we consider matrices of the form $A = (1, p, q)$ with integers $1 < p < q$ and p and q coprime, so that the toric ideal I_A is the ideal of a monomial smooth space curve in $\mathbb{C}^3$. The b–function $b_{A,\omega,\beta}(s)$ is denoted simply by $b_{\omega,\beta}(s)$ from now on. We refer to [22] for the main results on hypergeometric ideals and the corresponding b–functions $b_{\omega,\beta}(s)$ *for generic parameters* w *and* β (see below for details). In [19] the authors describe bounds for the roots of $b_{\omega,\beta}(s)$.

The first step is to describe the Gröbner fan of the toric ideal I_A ([13], [21]). We define a finite family of disjoint regions $R_i^{(k)}$ which are the intersection of two half-spaces with the line $(1, p, q)\mathbb{R}$ in common (see Example 1.3). The possible integers k and i depend on the extended Euclidean division of q over p.

Theorem 1.1. [13], [21] *We have*

$$\mathbb{R}^3 = \bigcup_{i,k} \overline{R_i^{(k)}}$$

and for each $\omega \in R_i^{(k)}$ *the initial ideal* $in_\omega(I_A)$ *is a monomial ideal and independent of* ω.

In [22] Theorem 3.1.3. was proved, under the assumption that the matrix A satisfies a homogeneity condition, that for generic values of the parameter β we have

$$in_{(-\omega,\omega)}(H_A(\beta)) = D_n \cdot in_\omega(I_A) + \sum_{1 \leq i \leq d} D_n \cdot (E_i - \beta_i)$$

This holds in our case too, and we describe explicitly the set of generic values of β.

In [22] Proposition 5.1.9. there is a description of $b_{\omega,\beta}(s)$ for Zariski generic β and generic ω (i.e. ω in the interior of any facet of the Gröbner fan of $H_A(\beta)$). In [5], $b_{\omega,\beta}(s)$ is described for $\omega = (1, 0, 0)$ and β generic. Our result is:

Theorem 1.2. *Given $R_i^{(k)}$, a facet of the Gröbner fan of I_A, there is a proper Zariski closed set $C_i^{(k)} \subset R_i^{(k)}$ such that if $\omega \in R_i^{(k)} \setminus C_i^{(k)}$ and β is generic the b–function is*

$$b_{\omega,\beta}(s) = \prod_{\alpha \in F_i^{(k)}} (s - \alpha)$$

for certain finite set $F_i^{(k)} \subseteq \mathbb{C}$. Moreover, if $\omega \in C_i^{(k)}$ or β is non-generic, then the reduced polynomial of the right hand side of previous equality gives a certain multiple of the b–function.

In the following example we sum up our results.

Example 1.3. Consider the matrix $A = (1, 3, 5)$. The Gröbner fan of $I_A \subset \mathbb{C}[\partial_x, \partial_y, \partial_z]$ consists of seven facets. Let us focus in one of them, namely $R_1^{(2)} = \{\omega \in \mathbb{R}^3 \mid 2\omega_1 + \omega_2 > \omega_3, \omega_1 + 3\omega_2 < 2\omega_3\}$. For any $\omega \in R_1^{(2)}$

$$in_\omega(I_A) = D\left(\partial_x^3, \partial_x^2\partial_y, \partial_x\partial_z, \partial_z^2\right).$$

Any complex number $\beta \neq 2$ is generic, and we have that

$$in_{(-\omega,\omega)}(H_A(\beta)) = D\left(\partial_x^2, \partial_x\partial_z, \partial_z^2, E - \beta\right).$$

We have $C_1^{(2)} = R_1^{(2)} \cap \{3\omega_1 + 4\omega_2 = 3\omega_3\}$. The b–function for $\omega \in R_1^{(2)} \setminus C_1^{(2)}$ and $\beta \neq 2$ is

$$b_{\omega,\beta}(s) = (s - \frac{\beta}{3}\omega_2)(s - \omega_1 - \frac{\beta - 1}{3}\omega_2)(s - \frac{\beta - 5}{3}\omega_2 - \omega_3).$$

If $\omega \in C_1^{(2)}$ and $\beta \neq 2$, the polynomial

$$(s - \frac{\beta}{3}\omega_2)(s - \omega_1 - \frac{\beta - 1}{3}\omega_2)$$

is a multiple of the b–function. With `Singular` we check that in this case we obtain the true b–function and not just a multiple. If $\omega \in R_1^{(2)}$ but $\beta = 2$ we have the following multiple of the b–function:

$$\begin{cases} (s - \frac{2}{3}\omega_2)(s - \omega_1 - \frac{1}{3}\omega_2)(s - 2\omega_1)(s + \omega_2 - \omega_3) & \text{if } \omega \notin C_1^{(2)} \\ (s - \frac{2}{3}\omega_2)(s - \omega_1 - \frac{1}{3}\omega_2)(s - 2\omega_1) & \text{otherwise.} \end{cases}$$

Again, with `Singular` we check that this is indeed $b_{\omega,2}(s)$. However, if we consider the region $R_2^{(2)} = \{\omega \in \mathbb{R}^3 \mid \omega_1 + 3\omega_2 > 2\omega_3, 3\omega_3 > 5\omega_2\}$, we have $\beta = 1, 2, 4, 7$ as non-generic values, and for $\omega \in R_2^{(2)}$ and $\beta = 2$ we give a polynomial with five roots, and only four of them are the roots of $b_{\omega,2}(s)$.

If $\omega \in \mathbb{R}^3 \setminus \bigcup_{i,k} R_i^{(k)}$ the study of $b_{\omega,\beta}(s)$ is a work in progress.

Acknowledgement. The authors would like to thank Daniel Andres, Viktor Levandovskyy and Jorge Martín-Morales for their useful comments and suggestions on this subject. This project started under the Spanish-German bilateral research project PRI-AIBOE-2011-0986. The authors are partially supported by MTM2013-40455-P and MTM2016-75024-P and Feder.

References

[1] Andres, D., Noncommutative Computer Algebra with Applications in Algebraic Analysis. Dissertation, Aachen (2014), `http://publications.rwth-aachen.de/record/228697/files/4928.pdf`.

[2] E. Artal Bartolo, Pi. Cassou-Noguès, I. Luengo, A. Melle-Hernández. *Bernstein polynomial of 2-Puiseux pairs irreducible plane curve singularities.* Methods and Applications of Analysis, Vol. 24, No. 2 (2017), pp. 185-214.

[3] Bernstein J. *Analytic continuation of generalized functions with respect to a parameter.* Funkcional. Anal. i Priložen. 6 (1972), no. 4, 26–40.

[4] Buchberger B. *An Algorithmical Criterion for the Solvability of Algebraic Systems of Equations (German)*, Aequationes Mathematicae **4**(3),(1970), 374–383.

[5] Fernández-Fernández, M.C. *Soluciones Gevrey de sistemas hypergométricos asociados a una curva monomial lisa.* DEA, U. Sevilla, 2008.

[6] Grayson D. and Stillman M. `Macaulay2`: *a software system for research in algebraic geometry.* Available at `http://www.math.uiuc.edu/Macaulay2` Leykin A., Tsai H. `D-modules` *package for* `Macaulay 2`. *Available at* `http://www.math. cornell.edu/~htsai`

[7] Decker W., Greuel G.-M., Pfister G., Schönemann, H.: Singular 4-1-1 — A computer algebra system for polynomial computations. http://www.singular.uni-kl.de (2018). Levandovskyy V., Martin-Morales J. `dmod.lib`. A Singular 4-1-1 library for Algorithms for algebraic D-modules.

[8] Hartillo-Hermoso M.I. *About an algorithm of T. Oaku.* in Ring Theory and Algebraic Geometry (León, 1999), 241–250, Lecture Notes in Pure and Appl. Math., 221, Dekker, New York, 2001.

[9] Kashiwara M. *B-functions and holonomic systems. Rationality of roots of B-functions.* Invent. Math. 38, 1 (1976) 33–53.

[10] Kashiwara M. *On the Holonomic Systems of Linear Differential Equations, II.* Inventiones math. 49, 121–135 (1978)

[11] Levandovskyy, V., Martín-Morales, J. *Algorithms for checking rational roots of b-functions and their applications.* J. Algebra 352 (2012), 408–429.

[12] Malgrange, M. *Le polynome de Bernstein d'une singularité isolée.* Lecture Notes in Math. 459, Springer, Berlin, 1975, 98-119.

[13] Mora, T., Robbiano, L. *The Gröbner fan of an ideal.* Computational aspects of commutative algebra. J. Symbolic Comput. 6 (1988), no. 2-3, 183–208.

[14] Noro M., Shimoyama T. and Takeshima T. *A Computer Algebra System* `Risa/Asir`. Available at `http://www.math.kobe-u.ac.jp/Asir/index.html`.

[15] Noro, M. An efficient modular algorithm for computing the global b-bunction. Mathematical software (Beijing, 2002), 147–157, World Sci. Publ., River Edge, NJ, 2002.

[16] Oaku T. *An algorithm of computing b -functions.* Duke Math. J. Volume 87, Number 1 (1997), 115–132.

[17] Oaku T. *Regular b -functions of D-modules.* J. Pure Appl.Algebra Volume 213, (2009), 1545–1557.

[18] Oaku T. and Takayama N. *Algorithms for D-modules – restriction, tensor product, localization, and local cohomology groups.* Journal of Pure and Applied Algebra, 156 (2001) pp. 495–518.

[19] Reichelt, T., Sevenheck, Ch., Walther, U. *On the b-functions of hypergeometric systems.* International Mathematics Research Notices, (2016)

[20] M. Sato. *Theory of prehomogeneous vector spaces (algebraic part)*—the English translation of Sato's lecture from Shintani's note. Notes by T. Shintani. Translated from the Japanese by M. Muro. Nagoya Math. J. 120 (1990), 1–34.

[21] Sturmfels, B., Gröbner bases and convex polytopes. University Lecture Series, 8. Providence RI, 1995.

[22] Saito M., Sturmfels B. and Takayama N. *Gröbner deformations of hypergeometric differential equations.* Algorithms and Computation in Mathematics, 6. Springer-Verlag, Berlin, (2000).

[23] Yano, T. *On the theory of b–functions.* Publ. RIMS, Kyoto Univ. 14, 111-202, 1978.

Departamento de Álgebra e IMUS. University of Seville. Spain
E-mail address: `castro@us.es, helenacobo@gmail.com`

Monografías de la Real Academia de Ciencias. Zaragoza. **43:** 71–74, (2018).
ISSN: 1132-6360

REGULARITY AND GRÖBNER BASES OF THE REES ALGEBRA OF EDGE IDEALS OF BIPARTITE GRAPHS

YAIRON CID-RUIZ

Abstract. Let G be a bipartite graph and $I = I(G)$ be its edge ideal. The aim of this note is to investigate different aspects of the Rees algebra $\mathcal{R}(I)$ of I. We compute its regularity and the universal Gröbner basis of its defining equations; interestingly, both of them are described in terms of the combinatorics of G.

We apply these ideas to study the regularity of the powers of I. For any $s \geq \operatorname{match}(G)+|E(G)|+1$ we prove that $\operatorname{reg}(I^{s+1}) = \operatorname{reg}(I^s)+2$ and that for an $s \geq 1$ we have the inequality $\operatorname{reg}(I^s) \leq 2s + \operatorname{match}(G) - 1$.

Let $G = (V(G), E(G))$ be a bipartite graph on the vertex set $V(G) = X \cup Y$ with bipartition $X = \{x_1, \ldots, x_n\}$ and $Y = \{y_1, \ldots, y_m\}$. Let $\mathbb{K}$ be a field and let R be the polynomial ring $R = \mathbb{K}[x_1, \ldots, x_n, y_1, \ldots, y_m]$. The edge ideal $I = I(G)$, associated to G, is the ideal of R generated by the set of monomials $x_i y_j$ such that x_i is adjacent to y_j.

One can find a vast literature on the Rees algebra of edge ideals of bipartite graphs (see see [28], [22], [11], [26], [25], [27], [10]), nevertheless, in this note we study several properties that might have been overlooked. From a computational point of view we first focus on the universal Gröbner basis of its defining equations, and from a more algebraic standpoint we focus on its total and partial regularities as a bigraded algebra. Applying these ideas, we give an estimation of when $\operatorname{reg}(I^s)$ starts to be a linear function and we find upper bounds for the regularity of the powers of I.

Let $\mathcal{R}(I) = \bigoplus_{i=0}^{\infty} I^i t^i \subset R[t]$ be the Rees algebra of the edge ideal I. Let $f_1, \ldots, f_q$ be the square free monomials of degree two generating I. We can see $\mathcal{R}(I)$ as a quotient of the polynomial ring $S = R[T_1, \ldots, T_q]$ via the map

$$\begin{aligned} S = \mathbb{K}[x_1, \ldots, x_n, y_1 \ldots, y_m, T_1, \ldots, T_q] &\xrightarrow{\psi} \mathcal{R}(I) \subset R[t], \\ \psi(x_i) = x_i, \quad \psi(y_i) = y_i, \quad \psi(T_i) &= f_i t. \end{aligned} \tag{1}$$

Then the presentation of $\mathcal{R}(I)$ is given by $S/\mathcal{K}$ where $\mathcal{K} = \operatorname{Ker}(\psi)$. We give a bigraded structure to $S = \mathbb{K}[x_1, \ldots, x_n, y_1, \ldots, y_m] \otimes_{\mathbb{K}} \mathbb{K}[T_1, \ldots, T_q]$, where $\operatorname{bideg}(x_i) = \operatorname{bideg}(y_i) = (1, 0)$ and $\operatorname{bideg}(T_i) = (0, 1)$. The map ψ from (1) becomes bihomogeneous when we declare $\operatorname{bideg}(t) = (-2, 1)$, then we have that $S/\mathcal{K}$ and $\mathcal{K}$ have natural bigraded structures as S-modules.

The universal Gröbner basis of the ideal $\mathcal{K}$ is defined as the union of all the reduced Gröbner bases $\mathcal{G}_<$ of the ideal $\mathcal{K}$ as $<$ runs over all possible monomial orders (see [23]). In our first main result we compute the universal Gröbner basis of the defining equations $\mathcal{K}$ of the Rees algebra $\mathcal{R}(I)$.

Theorem 1. *Let G be a bipartite graph and $\mathcal{K}$ be the defining equations of the Rees algebra $\mathcal{R}(I(G))$. The universal Gröbner basis $\mathcal{U}$ of $\mathcal{K}$ is given by*

$$\begin{aligned}\mathcal{U} = &\{T_w \mid w \text{ is an even cycle}\}\\ &\cup \{v_0T_{w^+} - v_aT_{w^-} \mid w = (v_0,\ldots,v_a) \text{ is an even path}\}\\ &\cup \{u_0u_aT_{(w_1,w_2)^+} - v_0v_bT_{(w_1,w_2)^-} \mid w_1 = (u_0,\ldots,u_a) \text{ and}\\ &\qquad\qquad w_2 = (v_0,\ldots,v_b) \text{ are disjoint odd paths}\}.\end{aligned}$$

From [25, Theorem 3.1, Proposition 3.1] we have a precise description of $\mathcal{K}$ given by syzygies of I and the set even of closed walks in the graph G. The algebra $\mathcal{R}(I)$, as a bigraded S-module, has a minimal bigraded free resolution

$$0 \longrightarrow F_p \longrightarrow \cdots \longrightarrow F_1 \longrightarrow F_0 \longrightarrow \mathcal{R}(I) \longrightarrow 0, \tag{2}$$

where $F_i = \oplus_j S(-a_{ij}, -b_{ij})$. In the same way as in [19], we can define the xy-regularity of $\mathcal{R}(I)$ by the integer

$$\operatorname{reg}_{xy}(\mathcal{R}(I)) = \max_{i,j}\{a_{ij} - i\},$$

or equivalently by

$$\operatorname{reg}_{xy}(\mathcal{R}(I)) = \max\{a \in \mathbb{Z} \mid \beta^S_{i,(a+i,b)}(\mathcal{R}(I)) \neq 0 \text{ for some } i, b \in \mathbb{Z}\},$$

where $\beta^S_{i,(a,b)}(\mathcal{R}(I)) = \dim_{\mathbb{K}}(\operatorname{Tor}^S_i(\mathcal{R}(I), \mathbb{K})_{(a,b)})$.

Similarly, we can define the T-regularity

$$\operatorname{reg}_T(\mathcal{R}(I)) = \max_{i,j}\{b_{ij} - i\}$$

and the total regularity

$$\operatorname{reg}(\mathcal{R}(I)) = \max_{i,j}\{a_{ij} + b_{ij} - i\}.$$

Our second main result is computing the total regularity and giving upper bounds for both partial regularities. The following is obtained by exploiting the canonical module of $\mathcal{R}(I)$ under the assumption of G being bipartite.

Theorem 2. *Let G be a bipartite graph. Then, we have:*

(i) $\operatorname{reg}(\mathcal{R}(I(G))) = \operatorname{match}(G)$,

(ii) $\operatorname{reg}_{xy}(\mathcal{R}(I(G))) \leq \operatorname{match}(G) - 1$,

(iii) $\operatorname{reg}_T(\mathcal{R}(I(G))) \leq \operatorname{match}(G)$,

where $\operatorname{match}(G)$ *denotes the matching number of* G.

Finally, we apply these results in order to study the regularity of the powers of the edge ideal $I = I(G)$.

It is a famous result (for a general ideal in a polynomial ring) the asymptotic linearity of $\operatorname{reg}(I^s)$ for $s \gg 0$ (see [8] and [18]). However, the exact form of this linear function and the exact point where $\operatorname{reg}(I^s)$ starts to be linear, is a problem that continues wide open even in the case of monomial ideals.

In recent years, a number of researchers have focused on computing the regularity of powers of edge ideals and on relating these values to combinatorial invariants of the graph (see e.g. [4], [1], [2], [3], [5], [17]). Most of the upper bounds given in these papers use the

concept of even-connection introduced in [3]. Actually, using this idea as a central tool, in [17] it was proved the upper bound

$$\operatorname{reg}(I^s) \leq 2s + \text{co-chord}(G) - 1$$

for any bipartite graph G, where co-chord(G) represents the co-chordal number of G (see [17, Definition 3.1]). From this nice result we get other sought upper bounds

$$\operatorname{reg}(I^s) \leq 2s + \text{co-chord}(G) - 1 \leq 2s + b(G) - 1 \leq 2s + \operatorname{match}(G) - 1,$$

where $b(G)$ represents the minimum cardinality of the maximal matchings of G and match(G) denotes the maximum cardinality of the matchings of G.

As a consequence of our study of the Rees algebra $\mathcal{R}(I)$, we make an estimation of when $\operatorname{reg}(I^s)$ starts to be a linear function, and we obtain the upper bound $\operatorname{reg}(I^s) \leq 2s + \operatorname{match}(G) - 1$. Perhaps, this could give new tools and fresh ideas to pursue the stronger and conjectured upper bound

$$\operatorname{reg}(I^s) \leq 2s + \operatorname{reg}(I) - 2.$$

From the characterization of the universal Gröbner basis and a special monomial order, we get the following results.

Corollary 3. *Let G be a bipartite graph with bipartition $V(G) = X \cup Y$. Then, for all $s \geq 1$ we have*

$$\operatorname{reg}(I(G)^s) \leq 2s + \min\big\{|X| - 1,\ |Y| - 1,\ 2b(G) - 1\big\}.$$

In the particular case of G being a complete bipartite graph we have

$$\operatorname{reg}(I(G)^s) = 2s.$$

Using the upper bounds for the partial regularities of $\mathcal{R}(I)$, we can get our last results.

Corollary 4. *Let G be a bipartite graph. Then, the following statements hold:*

(i) For all $s \geq \operatorname{match}(G) + |E(G)| + 1$ we have

$$\operatorname{reg}(I(G)^{s+1}) = \operatorname{reg}(I(G)^s) + 2.$$

(ii) For all $s \geq 1$ we have

$$\operatorname{reg}(I(G)^s) \leq 2s + \operatorname{match}(G) - 1.$$

References

[1] A. Alilooee, S. Beyarslan, and S. Selvaraja, *Regularity of Powers of Unicyclic Graphs*, ArXiv e-prints (February 2017), available at 1702.00916.

[2] Ali Alilooee and Arindam Banerjee, *Powers of edge ideals of regularity three bipartite graphs*, J. Commut. Algebra **9** (2017), no. 4, 441–454.

[3] Arindam Banerjee, *The regularity of powers of edge ideals*, J. Algebraic Combin. **41** (2015), no. 2, 303–321.

[4] Arindam Banerjee, Selvi Beyarslan, and Huy Tài Hà, *Regularity of edge ideals and their powers*, arXiv preprint arXiv:1712.00887 (2017).

[5] Selvi Beyarslan, Huy Tài Hà, and Trân Nam Trung, *Regularity of powers of forests and cycles*, J. Algebraic Combin. **42** (2015), no. 4, 1077–1095.

[6] Winfried Bruns and Joseph Gubeladze, *Polytopes, rings, and K-theory*, Springer Monographs in Mathematics, Springer, Dordrecht, 2009.

[7] Winfried Bruns and Jürgen Herzog, *Cohen-macaulay rings*, 2nd ed., Cambridge Studies in Advanced Mathematics, Cambridge University Press, 1998.
[8] S. Dale Cutkosky, Jürgen Herzog, and Ngô Viêt Trung, *Asymptotic behaviour of the Castelnuovo-Mumford regularity*, Compositio Math. **118** (1999), no. 3, 243–261.
[9] David Eisenbud, *Commutative algebra: with a view toward algebraic geometry*, Graduate Texts in Mathematics, vol. 150, Springer-Verlag, New York, 1995.
[10] Louiza Fouli and Kuei-Nuan Lin, *Rees algebras of square-free monomial ideals*, J. Commut. Algebra **7** (2015), no. 1, 25–54.
[11] Isidoro Gitler, Carlos Valencia, and Rafael H. Villarreal, *A note on the Rees algebra of a bipartite graph*, J. Pure Appl. Algebra **201** (2005), no. 1-3, 17–24.
[12] Daniel R. Grayson and Michael E. Stillman, *Macaulay2, a software system for research in algebraic geometry*, Available at http://www.math.uiuc.edu/Macaulay2/.
[13] Huy Tài Hà and Adam Van Tuyl, *Monomial ideals, edge ideals of hypergraphs, and their graded Betti numbers*, J. Algebraic Combin. **27** (2008), no. 2, 215–245.
[14] Jürgen Herzog and Takayuki Hibi, *Monomial ideals*, Graduate Texts in Mathematics, vol. 260, Springer-Verlag London, Ltd., London, 2011.
[15] Takayuki Hibi, Akihiro Higashitani, Kyouko Kimura, and Akiyoshi Tsuchiya, *Dominating induced matchings of finite graphs and regularity of edge ideals*, J. Algebraic Combin. **43** (2016), no. 1, 173–198.
[16] M. Hochster, *Rings of invariants of tori, Cohen-Macaulay rings generated by monomials, and polytopes*, Ann. of Math. (2) **96** (1972), 318–337.
[17] A. V. Jayanthan, N. Narayanan, and S. Selvaraja, *Regularity of powers of bipartite graphs*, Journal of Algebraic Combinatorics (2017May).
[18] Vijay Kodiyalam, *Asymptotic behaviour of Castelnuovo-Mumford regularity*, Proc. Amer. Math. Soc. **128** (2000), no. 2, 407–411.
[19] Tim Römer, *Homological properties of bigraded algebras*, Illinois J. Math. **45** (2001), no. 4, 1361–1376.
[20] Peter Schenzel, *On the use of local cohomology in algebra and geometry*, Six lectures on commutative algebra (Bellaterra, 1996), 1998, pp. 241–292.
[21] Aron Simis, Bernd Ulrich, and Wolmer V. Vasconcelos, *Rees algebras of modules*, Proc. London Math. Soc. (3) **87** (2003), no. 3, 610–646.
[22] Aron Simis, Wolmer V. Vasconcelos, and Rafael H. Villarreal, *On the ideal theory of graphs*, J. Algebra **167** (1994), no. 2, 389–416.
[23] Bernd Sturmfels, *Gröbner bases and convex polytopes*, University Lecture Series, vol. 8, American Mathematical Society, Providence, RI, 1996.
[24] Wolmer V. Vasconcelos, *Computational methods in commutative algebra and algebraic geometry*, Algorithms and Computation in Mathematics, vol. 2, Springer-Verlag, Berlin, 1998. With chapters by David Eisenbud, Daniel R. Grayson, Jürgen Herzog and Michael Stillman.
[25] Rafael H. Villarreal, *Rees algebras of edge ideals*, Comm. Algebra **23** (1995), no. 9, 3513–3524.
[26] ———, *Rees algebras of complete bipartite graphs*, Mat. Contemp. **16** (1999), 281–289. 15th School of Algebra (Portuguese) (Canela, 1998).
[27] ———, *Rees algebras and polyhedral cones of ideals of vertex covers of perfect graphs*, J. Algebraic Combin. **27** (2008), no. 3, 293–305.
[28] ———, *Monomial algebras*, Second, Monographs and Research Notes in Mathematics, CRC Press, Boca Raton, FL, 2015.

Department de Matemàtiques i Informàtica, Facultat de Matemàtiques i Informàtica, Universitat de Barcelona, Gran Via de les Corts Catalanes, 585; 08007 Barcelona, Spain.
E-mail address: ycid@ub.edu
URL: http://www.ub.edu/arcades/ycid.html

Monografías de la Real Academia de Ciencias. Zaragoza. **43:** 75–78, (2018).
ISSN: 1132-6360

RATIONAL INTERPOLATION AND THE EULER-JACOBI FORMULA

TERESA CORTADELLAS, CARLOS D'ANDREA, AND EULÀLIA MONTORO

Abstract. We generalize the Euler-Jacobi approach for the Rational Interpolation Problem given in [EK89] to the Rational Hermite Interpolation Problem and obtain an algorithm which works at a cost of $O(N \log^2 N)$, where $N+1$ is the sum of the multiplicities of the given points.

Introduction

Let $\mathbb{F}$ a field with $\mathrm{char}(\mathbb{F}) = 0$ and $(x_0, f_0; \ldots; x_N, f_N)$ a set of points in $\mathbb{F}$ with $x_i \neq x_j$, $i \neq j$. *The Rational Interpolation Problem* is the following: given $m, n \in \mathbb{N}$ with $n+m = N$, decide if there exists, and if so and compute two polynomials $p_m(x)$ and $q_n(x)$ of degrees bounded by m and n respectively, such that

$$\frac{p_m(x_i)}{q_n(x_i)} = f_i, \quad i = 0, \ldots, N. \tag{1}$$

In [EK89] an algorithm based on the Euler-Jacobi Formula to compute $p_m(x)$ and $q_n(x)$ with complexity $O(N^2)$ was proposed. We rewrite this algorithm using the language of residues. This will allow us to extend it to the Rational Hermite Interpolation, i.e. when the interpolation also takes into higher derivatives. We will focus in computing $q_n(x)$, the numerator $p_m(x)$ can be obtained with a similar method a posteriori.

Definition 0.1. Let $P(x), Q(x) \in \mathbb{F}[x]$, and $\sum_{n\in\mathbb{Z}} a_n(x-x')^n$ the Laurent series of $\frac{P(x)}{Q(x)}$ around $x = x'$.

(1) The local residue of $\frac{P(x)}{Q(x)}$ in $x = x'$ is

$$\mathrm{Res}_{x'}\left(\frac{P(x)}{Q(x)}\right) = a_{-1}.$$

(2) The global residue of $\frac{P(x)}{Q(x)}$ is

$$\mathrm{Res}_{glo}\left(\frac{P(x)}{Q(x)}\right) = \sum_{Q(x')=0} \mathrm{Res}_{x'}\left(\frac{P(x)}{Q(x)}\right).$$

Theorem 0.2. *(Euler-Jacobi) If* $P(x), Q(x) \in \mathbb{F}[x]$ *satisfy* $\deg(P(x)) \leq \deg(Q(x)) - 2$, *then*

$$\mathrm{Res}_{glo}\left(\frac{P(x)}{Q(x)}\right) = 0.$$

Let $f(x)$ be the unique polynomial of degree d bounded by N such that $f(x_i) = f_i$ (Lagrange polynomial) and $\omega(x) = (x-x_0)\ldots(x-x_N)$. We can consider a weak version

of (1): given $m, n \in \mathbb{N}$ with $n + m = N$, decide if there exist and compute two polynomials $p_m(x)$ and $q_n(x)$ of degrees bounded by m and n respectively, such that

$$p_m(x_i) = f_i q_n(x_i),\ i = 0, \ldots, N. \tag{2}$$

The weak problem implies

$$\mathrm{Res}_{glo}\left(\frac{x^j p_m(x)}{\omega(x)}\right) = \mathrm{Res}_{glo}\left(\frac{x^j f(x) q_n(x)}{\omega(x)}\right), \quad 0 \leq j \leq n-1.$$

Notice that $\deg(x^j p_m(x)) \leq j + m \leq n - 1 + m = N - 1 = \deg(\omega(x)) - 2$, then, as a consequence of the Euler-Jacobi formula

$$\mathrm{Res}_{glo}\left(\frac{x^j p_m(x)}{\omega(x)}\right) = 0.$$

Therefore, if we write $q_n(x) = \sum_{k=0}^{n} b_k x^k$ and $\omega'(x_i) = \omega_i$, we have that

$$0 = \mathrm{Res}_{glo}\left(\frac{x^j f(x) q_n(x)}{\omega(x)}\right) = \sum_{i=0}^{N}\sum_{k=0}^{n} \frac{x_i^j f(x_i) b_k x_i^k}{\omega_i} = \sum_{k=0}^{n}\left(\sum_{i=0}^{N} \frac{x_i^{j+k} f(x_i)}{\omega_i}\right) b_k.$$

If we denote $h_{j+k} = \sum_{i=0}^{N} \frac{x_i^{j+k} f(x_i)}{\omega_i}$, $0 \leq j \leq n-1$, the above equation can be written in matricial form as

$$\begin{pmatrix} h_0 & h_1 & \ldots & h_n \\ h_1 & h_2 & \ldots & h_{n+1} \\ \vdots & \vdots & \ldots & \vdots \\ h_{n-1} & h_n & \ldots & h_{2n-1} \end{pmatrix} \begin{pmatrix} b_0 \\ \vdots \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ \vdots \\ 0 \end{pmatrix}$$

Therefore to compute $q_n(x)$ is reduced to obtain one vector of $\ker H$ where $H = (h_s)_{0 \leq s \leq 2n-1}$. Notice that H is a Hankel matrix. Such matrices are a well-known structured matrices and compute its kernels is easy. Moreover in [EK89] the following lemma is obtained.

Lemma 0.3. *The cost of compute $H = (h_s)_{0 \leq s \leq 2n-1}$ is $O(N^2)$.*

In [EK89] assuming that $q_n(x)$ is a monic polynomial of degree n and that H is strongly non-singular, a Hankel system is solved directly using Trench algorithm [Tren65]. Without the hypothesis of non-singularity in [Gem93] there is an alternative algorithm. The total cost of all those algorithms is $O(n^2)$. Our goal is to generalize these results for the Hermite Rational Interpolation problem described below, and avoiding any assumption on the matrix H.

1. General Case

Let $(x_0, f_{0,0}, \ldots, f_{0,N_0-1}; \ldots; x_L, f_{L,0}, \ldots, f_{L,N_L-1})$ a set of points in $\mathbb{F}$ with $x_i \neq x_j$ if $i \neq j$. *The Rational Hermite Interpolation Problem* is the following: given $m, n \in \mathbb{N}$ with $n + m = N$ and $N + 1 = N_0 + \ldots + N_L$, decide if there exist and compute two polynomials $p_m(x)$ and $q_n(x)$ of degrees bounded by m and n respectively, such that

$$\left(\frac{p_m}{q_n}\right)^{(j)}(x_i) = f_{i,j}, \quad i = 0, \ldots, N_j - 1, \quad j = 0, \ldots, L. \tag{3}$$

Let $f(x)$ be the unique polynomial of degree d bounded by N such that $f^{(j)}(x_i) = f_{i,j}, \quad i = 0, \dots N_j - 1, \quad j = 0, \dots, L$ (Hermite polynomial) and $\omega(x) = (x - x_0)^{N_0} \dots (x - x_L)^{N_L}$. We can consider the weak version of (3): given $m, n \in \mathbb{N}$ with $n + m = N$ and $N + 1 = N_0 + \ldots + N_L$, decide if there exists and compute two polynomials $p_m(x)$ and $q_n(x)$ of degrees bounded by m and n respectively, such that

$$p_m^{(j)}(x_i) = \sum_{k=0}^{j} \binom{j}{k} f_{i,j} q_n^{(j-k)}(x_i),\ i = 0, \dots, N_j - 1, \quad j = 0, \dots, L. \tag{4}$$

Applying the same techniques used in the simple case, again the problem of computing $q_n(x)$ is reduced to obtain a vector of $\ker H$.

The following lemma is a consequence of this relation between global and local residue, for a rational function $R(x)$ we have that

$$\mathrm{Res}_{glo}\left(R(x)\right) = \mathrm{Res}_0\left(\frac{R(\frac{1}{x})}{x^2}\right).$$

Lemma 1.1. *Let $f^{\mathrm{rev}}(x) = x^d f(\frac{1}{x})$ and $\omega^{\mathrm{rev}}(x) = x^{N+1}\omega(\frac{1}{x})$ be the reversal polynomials of $f(x)$ and $\omega(x)$ respectively, then*

$$h_s = \mathrm{Res}_0\left(\frac{f^{\mathrm{rev}}(x)}{\omega^{\mathrm{rev}}(x) x^{1+s+d-N}}\right), 0 \le s \le 2n-1. \tag{5}$$

If we write

$$\frac{f^{\mathrm{rev}}(x)}{\omega^{\mathrm{rev}}(x)} = f^{\mathrm{rev}}(x) \prod_{i=0}^{L} \sum_{j=0}^{\infty} \frac{j(j-1)\dots(j-N_i)}{(N_i-1)!} (x_i x)^{j-N_i+1}$$

and $M = 1 + s + d - N$, then the local residue in 0 is the coefficient of degree $M - 1$ of the above series.

An alternative way to compute it is the following

$$\mathrm{Res}_0\left(\frac{\frac{f^{\mathrm{rev}}(x)}{\omega^{\mathrm{rev}}(x)}}{x^{1+s+d-N}}\right) = \lim_{x\to 0} \frac{1}{(M-1)!} \frac{d^{M-1}}{dx^{M-1}} \left(x^M \frac{f^{\mathrm{rev}}(x)}{\omega^{\mathrm{rev}}(x)}\right).$$

None of two above formulas is computationally efficient. In what follows we present a more efficient method.

To compute $H = (h_s)_{0 \le s \le 2n-1}$, with

$$h_s = \mathrm{Res}_0\left(\frac{f^{\mathrm{rev}}(x)}{\omega^{\mathrm{rev}}(x) x^{1+s+d-N}}\right),$$

we can use the Extended Euclidean Algorithm in the following form:

$$\omega^{\mathrm{rev}}(x) G_s(x) + x^{1+s+d-N} H_s(x) = 1 \Rightarrow \frac{1}{\omega^{\mathrm{rev}}(x)} = G_s(x) + \frac{x^{2+s+d-N} H_s(x)}{\omega^{\mathrm{rev}}(x)}$$

with $\deg G_s(x) < 1 + s + d - N$ and $\deg H_s(x) < N + 1$.

Therefore:

$$h_s = \mathrm{Res}_0\left(\frac{f^{\mathrm{rev}}(x)G_s(x)}{x^{1+s+d-N}} + \frac{f^{\mathrm{rev}}(x)H_s(x)}{\omega^{\mathrm{rev}}(x)}\right) = \mathrm{Res}_0\left(\frac{f^{\mathrm{rev}}(x)G_s(x)}{x^{1+s+d-N}}\right)$$

Next lemma is a consequence to the fact that we only need just one computation to obtain an optimal cost.

Lemma 1.2. *If $n \leq \frac{N}{2}$, the cost of computing the matrix $H = (h_s)_{0\leq s\leq 2n-1}$ is $0(N\log^2 N)$.*

To compute one vector of $\ker H$, again we use Extended Euclidean Algorithm. In particular, we apply this algorithm to $h(x) = h_{2n-1} + h_{2n-2}x + \ldots + h_0x^{2n-1}$ and $r_0(x) = x^{2n}$ (see [Bin94, vzGG13]) and we obtain the following:

Proposition 1.3. *The cost of computing one vector of* $\ker H$ *is $O(n\log^2 n)$.*

As a conclusion, taking into account the previous results we have the following theorem.

Theorem 1.4. *The Euler-Jacobi method can be extended to the case of multiplicities, and the Rational Hermite Interpolation Problem can be solved at cost $O(N\log^2 N)$.*

Acknowledgements T. Cortadellas is supported by the Spanish MEC research project MTM2013-40775-P, C. D'Andrea and E. Montoro are supported by the Spanish MINECO/ FEDER research project MTM 2015-65361-P. C. D'Andrea is also supported by the "María de Maeztu" Programme for Units of Excellence in R&D (MDM-2014-0445). E. Montoro is also supported by MTM2017-90682-REDT.

References

[Bin94] Bini, Dario and Pan, Victor. *Polynomial and Matrix Computations. Vol 1* Birkhausser Boston, 1994.

[EK89] Eğecioğlu, Ömer; Koç, Çetin K. *A fast algorithm for rational interpolation via orthogonal polynomials.* Math. Comp. 53 (1989), no. 187, 249–264.

[Gem93] Gemignani, Luca. *Rational interpolation via orthogonal polynomials.* Comput. Math. Appl. 26 (1993), no. 5, 27–34.

[Tren65] Trench, W.F. *An algorithm for the inversion of finite Hankel matrices.* J. Soc. Indust. Appl. Math., v. 13 (1965), pp. 1102–1107.

[vzGG13] Von zur Gathen, Joachim; Gerhard, Jürgen. *Modern computer algebra.* Third edition. Cambridge University Press, Cambridge, 2013.

Universitat de Barcelona, Facultat de Educació. Passeig de la Vall d'Hebron 171, 08035 Barcelona, Spain

E-mail address: terecortadellas@ub.edu

Universitat de Barcelona, Departament de Matemàtiques i Informàtica, Gran Via de les Corts Catalanes 585, 08007 Barcelona, Spain

E-mail address: cdandrea@ub.edu http://www.ub.edu/arcades/cdandrea.html

Universitat de Barcelona, Departament de Matemàtiques i Informàtica, Gran Via de les Corts Catalanes 585, 08007 Barcelona, Spain

E-mail address: eula.montoro@ub.edu

Monografías de la Real Academia de Ciencias. Zaragoza. **43:** 79–82, (2018).
ISSN: 1132-6360

THE MINIMAL SOLUTIONS OF THE RATIONAL INTERPOLATION PROBLEM

TERESA CORTADELLAS, CARLOS D'ANDREA, AND EULÀLIA MONTORO

Abstract. We look for minimal solutions of the rational interpolation problem $y^{(j)}(x_i) = y_{i,j}$ in terms of two different degrees. The space of rational functions $y = \frac{a}{b}$ interpolating a given set of points can be parameterized keeping track the degrees $\delta(y) = \max\{\deg a, \deg b\}$ and $\kappa(y) = \deg a + \deg b$. In both cases the minimal solutions, the rational interpolating functions with smallest degree, can be expressed in terms of the Euclidean algorithm. We review these results and prove those related with the δ degree in the framework of syzygies.

Introduction

Let $\mathbb{K}$ be a field of characteristic zero, $l, n_1, \dots, n_l$ positive integers, $n := n_1 + \cdots + n_l$, and a set of n pairs of elements of $\mathbb{K}$

$$(x_i, y_{i,j}), \text{ for } i = 1, \dots l, \quad j = 0, \dots n_i - 1 \tag{1}$$

with the x_i's distinct.

An interpolating rational function of this data is a rational function $y(x)$ satisfying

$$y^{(j)}(x_i) = y_{i,j}, \qquad i = 1, \dots l, \quad j = 0, \dots n_i - 1. \tag{2}$$

The rational interpolation problem is to find all the interpolating rational functions of a given data. We will refer to the case without multiplicities (that is, the case $n_i = 1$) as the "classical rational interpolation problem".

The degree of a rational function $y(x) = \frac{a(x)}{b(x)}$, with $a(x), b(x)$ polynomials in $\mathbb{K}[x]$, can be defined, among others, as

$$\begin{aligned} &\delta(y) = \max\{\deg a(x), \deg b(x)\}, \text{ and} \\ &\kappa(y) = \deg a(x) + \deg b(x). \end{aligned}$$

Fixed a rational function degree, we say that m is an admissible degree if there exists an interpolating function of degree m. A natural question to ask is which numbers are admissible, in particular to characterize the smallest of them, and fixed an admissible integer to parametrize all the corresponding rational functions. These questions are solved in [AntAn86] for δ and, in [Ant88] for κ. The main tool in the first mentioned paper is a divided-differences matrix whereas in the second is the Euclidean algorithm. Later, in [ABKW90] the solutions of the classical rational interpolation problem are given as the kernel of a matrix encoding the data of the problem. In [Ra97] this matrix is homogenized and then, the numerical invariants of minimal free resolutions can be used to tackle the problem.

Let us denote by $g(x)$ the Hermite polynomial of (1); that is, the unique interpolating polynomial of the data of degree less than n, and $m(x) = (x - x_1)^{n_1} \cdots (x - x_l)^{n_l}$.

We use the framework of syzygies and the δ degree to give a minimal basis of the set of pairs of polynomials $(a(x), b(x))$ verifying the interpolating conditions. We show how the Euclidean algorithm for $m(x)$ and $g(x)$ gives such a minimal basis. This algorithm also allows to parameterize all rational interpolating functions following the κ degree. The Hermite rational interpolation problem consists in deciding if there exist, and if so compute, polynomials $a(x), b(x)$ of degrees bounded by a $(0 \leq a < n)$ and $n - a - 1$ such that $\frac{a(x)}{b(x)}$ interpolates the data. We treat this problem making use of the results for the κ degree.

1. The degree δ

Any interpolating function $y(x) = \frac{a(x)}{b(x)}$ satisfies

$$(a(x) - b(x)g(x))^{(j)}(x_i) = 0, \quad i = 1, \dots l, \quad j = 0, \dots n_i - 1; \tag{3}$$

equivalently, there exists a polynomial $c(x)$ such that

$$a(x) = b(x)g(x) + c(x)m(x). \tag{4}$$

We will refer, indistinctly, to (3) or (4) as the weak interpolation conditions.

In fact, a rational fraction $y(x) = \frac{a(x)}{b(x)}$ is an interpolating function if and only if the pair $(a(x), b(x))$ satisfies the weak interpolation conditions and $b(x_i) \neq 0$, for $i = 1, \dots, l$.

We observe that$(a(x), b(x), c(x)) \in \mathbb{K}[x]^3$ is an element of the kernel of the morphism of $\mathbb{K}[x]$-modules $\varphi : \mathbb{K}[x]^3 \longrightarrow \mathbb{K}[x]$ with associated matrix, in the canonical basis, given by

$$\begin{pmatrix} 1 & -g(x) & -m(x) \end{pmatrix},$$

and that the set $Y = \{(a(x), b(x)) \text{ such that } a(x) - b(x)g(x) \in m(x)\mathbb{K}[x]\}$ of pairs of polynomials which satisfy the weak interpolating conditions, is a free $\mathbb{K}[x]$-module of rank 2.

Homogenizing the above situation in $\mathbb{K}[x, z]$ one obtains a homogeneous morphism $\phi : \mathbb{K}[x, z](-n)^3 \longrightarrow \mathbb{K}[x, z]$ given by the matrix

$$\begin{pmatrix} z^n & -g(x, z) & -m(x, z) \end{pmatrix},$$

and a minimal free resolution of $\mathbb{K}[x, z]/\text{Coker}(\phi)$

$$0 \longrightarrow \mathbb{K}[x, z](-n - \delta_1) \oplus \mathbb{K}[x, z](-n - \delta_2) \longrightarrow \mathbb{K}[x, z](-n)^3 \longrightarrow \mathbb{K}[x, z]$$

with $\delta_1 + \delta_2 = n$ and $\delta_1 \leq \delta_2$.

Definition 1.1. We say that a basis $(a_1(x), b_1(x))$, $(a_2(x), b_2(x))$ of Y is a minimal basis if $\delta(\frac{a_1(x)}{a_1(x)}) = \max\{\deg a_1(x), \deg b_1(x)\}) = \delta_1$ and $\delta(\frac{a_2(x)}{a_2(x)}) = \max\{\deg a_2(x), \deg b_2(x)\} = \delta_2$.

The following is our main theorem (see [AntAn86, Theorem 2.11]).

Theorem 1.2. *Let $(a_1(x), b_1(x))$, $(a_2(x), b_2(x))$ be a minimal basis of Y. The rational function $y(x)$ is an interpolating function if, and only if, there exist polynomials $p(x)$ and $q(x)$ such that*

$$y(x) = \frac{p(x)a_1(x) + q(x)a_2(x)}{p(x)b_1(x) + q(x)b_2(x)}$$

and $p(x_i)b_1(x_i) + q(x_i)b_2(x_i) \neq 0$ for $i = 1, \ldots, l$.

If $a_1(x)$ and $b_1(x)$ are coprime, and $\delta_1 < \delta_2$, then there is a unique interpolating function $y_{\min}(x)$ of minimal degree

$$y_{\min}(x) = \frac{a_1(x)}{b_1(x)}.$$

Otherwise, if either $a_1(x)$ and $a_2(x)$ are not coprime, or $\delta_1 = \delta_2$, then there is a family of interpolating functions of minimal degree which can be parametrized as

$$y_{\min}(x) = \frac{a_2(x) + p(x)a_1(x)}{b_2(x) + p(x)b_1(x)},$$

where $\deg p(x) = \delta_2 - \delta_1$, and $b_2(x_i) + p(x_i)b_1(x_i) \neq 0$, $i = 1, \ldots, l$.

As a corollary the minimal admissible degree is δ_1 or δ_2 and any degree above δ_2 is admissible.

Put $r_0 = m(x)$, $r_1 = g(x)$. Following the Euclidean algorithm, there exists a positive integer N and unique nonzero polynomials such that

$$r_i = q_{i+1}r_{i+1} + r_{i+2}, \qquad i = 0, \ldots, N-1, \quad r_{N+1} = 0$$

and $\deg r_i > \deg r_{i+1}$, $i = 1, \ldots N$.

Using the quotients one defines recursively two sequences of polynomials s_i, t_i, for $i = 0, \ldots, N+1$, satisfying $r_i = r_1 s_i + r_0 t_i$, $\quad i = 0, \ldots N+1$. For each i the pair (r_i, s_i), (r_{i+1}, s_{i+1}) is a basis of Y an there exists an index for which the pair is a minimal basis.

Example 1.3. In the generic case; that is, if the quotients in the Euclidean algorithm have degree one, then $N = n$, $\deg r_i = n - i$ for $i = 1, \ldots, n$ and $\deg s_i = i - 1$ for $i = 2, \ldots n$.

(a) If $n = 2k$ then $(r_k, s_k), (r_{k+1}, s_{k+1})$ is a minimal basis and the minimal degree is k.
(b) If $n = 2k + 1$ then $(r_k, s_k), (r_{k+1}, s_{k+1})$ and $(r_{k+1}, s_{k+1}), (r_{k+2}, s_{k+2})$ are minimal basis and the minimal degree is k or $k + 1$.

2. The degree κ

With the notations introduced in the above sections, the two following results are obtained in [Ant88, Theorem 3.2 and Corrollary 3.5].

Theorem 2.1. *For every rational function $y(x)$ there exists a unique set of polynomial $m_0(x), \ldots, m_{N+1}(x)$ such that*

$$y(x) = \frac{\sum_{i=0}^{N+1} m_i(x)r_i(x)}{\sum_{i=0}^{N+1} m_i(x)s_i(x)}, \text{ with } \deg m_i(x) < \deg q_i(x) \text{ for } i = 1, \ldots, N$$

and $\sum_{i=0}^{N+1} m_i(x_j)s_i(x_j) \neq 0$ for $j = 1, \ldots l$.

Corollary 2.2. *Put $\mu_i = \deg(q_i(x))$.*

(1) *The admissible $\kappa < n$ are in the set $\{n-\mu_1,\dots,n-\mu_N\}$. Moreover, $n-\mu_i$ is admissible iff $s_i(x_j)\neq 0$ for $j=1,\dots,l$; in this case $\kappa(\frac{r_i}{s_i}) = n-\mu_i$. The minimal degree is $n-\mu_{max}$ where $\mu_{max} = \max_i(\mu_i$ with $s_i(x_j)\neq 0$ for $j=1,\dots,l)$.*
(2) *n is admissible. The interpolating rational functions of degree n can be parametrized as $\frac{r_i+mr_{i+1}}{s_i+ms_{i+1}}$, with m constant such that $s_i(x_j)+ms_{i+1}(x_j)\neq 0$ for $j=1,\dots,l$, $i=0,\dots,N$. All integers greater than n are admissible.*
(3) *$n-1$ is admissible (that is the Cauchy interpolation problem is solvable) if and only if $\mu_i = 1$ for some $i=1,\dots,N$ provided that $s_i(x_j)\neq 0$ for $j=1,\dots,l$.*

Example 2.3. In the generic case the minimal degree is $n-1$, $g(x)$ is a minimal solution, $\frac{r_i}{s_i}$, for $i=1,\dots,n$, have degree $n-1$ and are minimal solutions if r_i and s_i are coprime.

Let $0\leq a\leq n-1$. We obtain the solution of the rational Hermite interpolation problem for a (see [CDM18, Theorem 2.6] and [vzGG13, Exercise 5.42]) as a consequence of the theorem 2.1.

Corollary 2.4. *Let $1\leq k\leq N$ such that*

$$\deg(r_k(x)) = n-(\mu_1+\cdots+\mu_k)\leq a < \deg(r_{k-1}(x)) = n-(\mu_1+\cdots+\mu_{k-1}).$$

Any solution of the Hermite interpolation problem for the integer a is $\frac{m(x)r_k(x)}{m(x)s_k(x)}$ for some $m(x)$. The problem has solution if and only if $r_k(x)$ and $s_k(x)$ are coprimes.

Acknowledgments T. Cortadellas is supported by the Spanish MEC research project MTM2013-40775-P, C. D'Andrea and E. Montoro by the Spanish MINECO/FEDER research project MTM 2015-65361-P. C. D'Andrea is also supported by the "María de Maeztu" Programme for Units of Excellence in R&D (MDM-2014-0445). E. Montoro is also supported by MTM2017-90682-REDT.

References

[AntAn86] Antoulas, A.C.; Anderson, B. D. Q. *On the Scalar Rational Interpolation Problem.* IMA Journal of Mathematical Control & Information 3 (1986), 61–88.
[Ant88] Antoulas, A.C. *Rational interpolation and the Euclidean algorithm.* Linear Algebra Appl. 188 (1988), 157–171.
[ABKW90] Antoulas, A.C.; Ball J.A.; Kang J.; Willens J.C. *On the Solution of the Minimal Rational Interpolation Problem.* Linear Algebra Appl. 137/138 (1990), 511–573.
[CDM18] Cortadellas Benítez, T.: D'Andrea, C.; Montoro, E. *The set of unattainable points for the rational Hermite interpolation problem.* Linear Algebra Appl. 538 (2018), 116—142.
[Ra97] Ravi, M. S. *Geometric methods in Rational Interpolation Theory.* Linear Algebra and its aplications. 258 (1997), 159–168.
[vzGG13] Von zur Gathen, Joachim; Gerhard, Jürgen. *Modern computer algebra.* Third edition. Cambridge University Press, Cambridge, 2013.

Universitat de Barcelona, Facultat d'Educació. Passeig de la Vall d'Hebron 171, 08035 Barcelona.
E-mail address: terecortadellas@ub.edu

Universitat de Barcelona, Facultat de Matemàtiques i Informàtica. Gran Via de les Corts Catalanes 585, 08007 Barcelona, Spain.
E-mail address: cdandrea@ub.edu

Universitat de Barcelona, Facultat de Matemàtiques i Informàtica. Gran Via de les Corts Catalanes 585, 08007 Barcelona, Spain.
E-mail address: eula.montoro@ub.edu

Monografías de la Real Academia de Ciencias. Zaragoza. **43:** 83–86, (2018).
ISSN: 1132-6360

COMPUTING MINIMAL GORENSTEIN COVERS OF ARTIN RINGS OF LOW GORENSTEIN COLENGTH

J. ELIAS AND R. HOMS

Abstract. Given a local Artin $\mathbf{k}$-algebra $A = \mathbf{k}[\![x_1, \dots x_n]\!]/I$, we are interested in providing minimal Gorenstein covers $G = \mathbf{k}[\![x_1, \dots x_n]\!]/J$. Our main goal is to effectively compute the variety of minimal Gorenstein covers of A for low Gorenstein colength.

Introduction

The Gorenstein colength $\operatorname{gcl}(A)$ of a local Artin $\mathbf{k}$-algebra $A = \mathbf{k}[\![x_1, \dots x_n]\!]/I$, where $\mathbf{k}$ is an arbitrary field, is defined by Ananthnarayan in [1] as the minimum $\ell(G) - \ell(A)$, where G is an Artin Gorenstein ring such that $A \simeq G/H$ for some ideal $H \subset G$. In [5] we approach the problem of computing the Gorenstein colength by characterizing algebras with $\operatorname{gcl}(A) \leq 2$ in terms of their Macaulay inverse system.

If $\operatorname{gcl}(A) = 1$, the Teter variety introduced in [6] is precisely the variety of all minimal Gorenstein covers of A. Here we extend this notion to the variety of minimal Gorenstein covers $MGC(A)$ of an Artin algebra A with arbitrary Gorenstein colength t. We provide some effective methods to compute explicitly $MGC(A)$ for low colength based on the integration method for inverse systems proposed by Mourrain in [7].

Set $R = \mathbf{k}[\![x_1, \dots x_n]\!]$ and $S = \mathbf{k}[y_1, \dots, y_n]$. S can be regarded as an R-module by contraction:

$$\begin{array}{ccccc} R \times S & \longrightarrow & S & & \\ (x^\alpha, y^\beta) & \mapsto & x^\alpha \circ y^\beta = & \left\{ \begin{array}{ll} y^{\beta-\alpha} & \beta \geq \alpha, \\ 0, & \text{otherwise.} \end{array} \right. \end{array}$$

The sub-R-module $I^\perp = \{g \in S \mid I \circ g = 0\}$ of S is called the Macaulay inverse system of $A = R/I$. Moreover, $A = R/I$ is Gorenstein of socle degree s if and only if $I^\perp$ is a cyclic R-module generated by a polynomial F of degree s. We denote this module by $\langle F \rangle$ and it is equal to the $\mathbf{k}$-vector space $\langle x^\alpha \circ F : |\alpha| \leq s \rangle_{\mathbf{k}}$.

Definition 0.1 (Minimal Gorenstein cover)**.** We say that $G = R/J$, with $J = \operatorname{Ann}_R F$, is a minimal Gorenstein cover of $A = R/I$ if and only if $I^\perp \subset \langle F \rangle$ and $\ell(G) = \ell(A) + \operatorname{gcl}(A)$.

We perform the computations of this paper with Singular [3], using the library [4] for inverse system related computations and a specifically created library for integrals and varieties $MGC(A)$. See [1], [2], [6] and [5] for more results on Teter rings, Gorenstein colength and related problems.

1. Gorenstein covers and integrals

The following result from [5] provides the exact relation between the inverse systems of $G = R/J$ and $A = R/I$ whenever G is a minimal Gorenstein cover of A expressed by the quotient ideal $K_F := (I^\perp :_R F)$, where $\langle F \rangle = J^\perp$.

Proposition 1.1. *Let $A = R/I$ be a local Artin algebra and $G = R/J$, with $J = \operatorname{Ann}_{\mathrm{R}} F$, a minimal Gorenstein cover of A. Then,*

(i) $I^\perp = K_F \circ F$,
(ii) $\operatorname{gcl}(A) = \ell(R/K_F)$.

Moreover, after a linear isomorphism of R we may assume:

$$K_F = \begin{cases} R & \text{if} \quad \operatorname{gcl}(A) = 0 \\ \mathfrak{m} & \text{if} \quad \operatorname{gcl}(A) = 1 \\ (x_1, \dots, x_{n-1}, x_n^2) & \text{if} \quad \operatorname{gcl}(A) = 2 \end{cases}$$

Therefore, given an inverse system $I^\perp$, in order to find a polynomial F defining a Gorenstein cover with the required colength, in case it exists, we need an inverse operation to contraction.

Definition 1.2 (Integral of a module with respect to an ideal)**.** Consider an R-module M of S. We define the integral of M with respect to the ideal K, denoted by $\int_K M$, as

$$\int_K M = \{G \in S \mid K \circ G \subset M\}.$$

By definition of the integral, clearly $F \in \int_{K_F} I^\perp$. However, K_F depends on F whenever $\operatorname{gcl}(A) \geq 2$ and therefore we need to remove this dependence by giving a bigger R-module where the covers lay.

Proposition 1.3. *Given a ring $A = R/I$ of Gorenstein colength t and a minimal Gorenstein cover $G = R/\operatorname{Ann}_{\mathrm{R}} F$ of A,*

(i) $F \in \int_{\mathfrak{m}^t} I^\perp$;
(ii) *for any $H \in \int_{\mathfrak{m}^t} I^\perp$, the condition $I^\perp \subset \langle H \rangle$ does not depend on the representative of the class $\overline{H}$ in $\dfrac{\int_{\mathfrak{m}^t} I^\perp}{I^\perp}$.*

In particular, any $F' \in \int_{\mathfrak{m}^t} I^\perp$ such that $\overline{F'} = \overline{F}$ in $\dfrac{\int_{\mathfrak{m}^t} I^\perp}{I^\perp}$ defines the same minimal Gorenstein cover $G = R/\operatorname{Ann}_{\mathrm{R}} F$.

A generalization of the work of Mourrain in [7] on an integration method to compute the inverse system $I^\perp$ provides an effective algorithm for computing a $\mathbf{k}$-basis of $\int_{\mathfrak{m}^t} I^\perp$ based on the following result:

Theorem 1.4. *Consider a sub-R-module M of S and $d \geq 1$. Let $\{b_1, \dots, b_{t_{d-1}}\}$ be a $\mathbf{k}$-basis of $\int_{\mathfrak{m}^{d-1}} M$ and let Λ be a polynomial with no constant terms. Then $\Lambda \in \int_{\mathfrak{m}^d} M$ if and only if it is of the form*

$$\Lambda = \sum_{j=1}^{t_{d-1}} \lambda_j^1 \int_1 b_j|_{y_2=\cdots=y_n=0} + \sum_{j=1}^{t_{d-1}} \lambda_j^2 \int_2 b_j|_{y_3=\cdots=y_n=0} + \cdots + \sum_{j=1}^{t_{d-1}} \lambda_j^n \int_n b_j, \quad \lambda_j^k \in \mathbf{k}, \tag{1}$$

such that

$$\sum_{j=1}^{t_{d-1}} \lambda_j^k (x_l \circ b_j) - \sum_{j=1}^{t_{d-1}} \lambda_j^l (x_k \circ b_j) = 0, 1 \leq k < l \leq n. \tag{2}$$

2. Variety of Minimal Gorenstein Covers

The following theorem proves the existence of the variety associated to $A = R/I$ whose closed points correspond to the minimal Gorenstein covers of A.

Theorem 2.1. *Let $A = R/I$ be an Artin ring of Gorenstein colength t. There exists a quasi-projective sub-variety $MGC(A)$ of $\mathbb{P}_{\mathbf{k}}\left(\frac{\int_{\mathfrak{m}^t} I^\perp}{I^\perp}\right)$, whose set of closed points are the points $[\overline{F}]$, $\overline{F} \in \int_{\mathfrak{m}^t} I^\perp/I^\perp$, such that $G = R/\operatorname{Ann}_{\mathrm{R}} F$ is a minimal Gorenstein cover of A.*

Definition 2.2. Given an Artin ring $A = R/I$ of Gorenstein colength t, we call $MGC(A)$ the minimal Gorenstein covers variety associated to A.

As for the effective computation of such object, we need to use the specific form of the quotient ideal K_F, which is available to us in the low colength case, that is, $\operatorname{gcl}(A) \leq 2$. The next result is the basis for an algorithm computing $MCG(A)$ when $\operatorname{gcl}(A) = 1$.

Proposition 2.3. *Let $A = R/I$ be a non-Gorenstein local Artin ring of socle degree s. Then $\operatorname{gcl}(A) = 1$ if and only if there exist a polynomial $F = \sum_{j=1}^{h} a_j F_j \in \int_{\mathfrak{m}} I^\perp$, where $\overline{F_1}, \ldots, \overline{F_h}$ is a $\mathbf{k}$-basis of $\frac{\int_{\mathfrak{m}} I^\perp}{I^\perp}$, such that $\dim_{\mathbf{k}}(\mathfrak{m} \circ F) = \dim_{\mathbf{k}} I^\perp$.*

Let us now provide a sketch of the algorithm used to compute the $MCG(A)$ of an Artin local algebra $A = R/I$, $n \geq 2$, of Gorenstein colength 1. The output of the algorithm is an homogeneous ideal $\mathfrak{a} \subset \mathbf{k}[a_1, \cdots, a_h]$ such that if $\mathfrak{a} = (0)$, then $\operatorname{gcl}(A) > 1$. Otherwise, $\operatorname{gcl}(A) = 1$ and

$$MGC(A) = \mathbb{P}^{h-1}_{\mathbf{k}} \setminus V_+(\mathfrak{a}).$$

Algorithm to compute $MGC(A)$ when $\operatorname{gcl}(A) = 1$
Input:

- $\mathbf{k}$-basis $b_1, \ldots, b_t$ of the inverse system $I^\perp$;
- polynomials $F_1, \ldots, F_h$ such that $\overline{F_1}, \ldots, \overline{F_h}$ is a $\mathbf{k}$-basis of $\int_{\mathfrak{m}} I^\perp/I^\perp$.

Output:

- ideal $\mathfrak{a} \subset \mathbf{k}[a_1, \cdots, a_h]$.

Steps:

(1) Define $F = a_1F_1 + \cdots + a_hF_h$, where $a_1, \ldots, a_h$ are variables in $\mathbf{k}$.
(2) Build matrix $A = \left(\mu_j^\alpha\right)_{1 \leq |\alpha| \leq s+1, 1 \leq j \leq t}$, where $x^\alpha \circ F = \sum_{j=1}^{t} \mu_j^\alpha b_j$.
(3) Compute the ideal $\mathfrak{a}$ generated by all minors of order t of the matrix A.

Example 2.4. Consider $A = \mathbf{k}[\![x_1, x_2]\!]/(x_1^2, x_1x_2, x_2^4)$, $\operatorname{gcl}(A) = 1$. In this case we have $\mathbb{P}_{\mathbf{k}}(\int_{\mathfrak{m}} I^\perp/I^\perp) = \mathbb{P}^2_{\mathbf{k}}$, a closed point $p = (a_1 : a_2 : a_3) \in \mathbb{P}^2_{\mathbf{k}}$ corresponds to a polynomial $F = a_1y_2^4 + a_2y_1y_2 + a_3y_1^2 \in \int_{\mathfrak{m}} I^\perp/I^\perp$. The algorithm outputs $\mathfrak{a} = (a_1a_3)$, so

$$MCG(A) = \mathbb{P}^2_{\mathbf{k}} \setminus V_+(\mathfrak{a}).$$

Now we state an analogous result for $\operatorname{gcl}(A) = 2$ that gives us the necessary background to design the algorithm to compute $MGC(A)$ in colength 2:

Proposition 2.5. *Given a non-Gorenstein non-Teter local Artin ring $A = R/I$, $\operatorname{gcl}(A) = 2$ if and only if there exist a polynomial $F = \sum_{i=1}^{2}\sum_{j=1}^{h} a_j^i F_j^i \in \int_{\mathfrak{m}^2} I^\perp$, where $\overline{F_1^i}, \dots, \overline{F_h^i}$ is a $\mathbf{k}$-basis of $\frac{\int_{\mathfrak{m}^i} I^\perp}{\int_{\mathfrak{m}^{i-1}} I^\perp}$, $i = 1, 2$, such that $(L_1, \dots, L_{n-1}, L_n^2) \circ F = I^\perp$ for suitable independent linear forms L_i.*

Example 2.6. Consider $A = \mathbf{k}[\![x_1, x_2]\!]/(x_1^2, x_1x_2^2, x_2^4)$, $\operatorname{gcl}(A) = 2$. We have $\mathbb{P}_{\mathbf{k}}(\int_{\mathfrak{m}^2} I^\perp/I^\perp) = \mathbb{P}^6_{\mathbf{k}}$, a closed point $p = (a_1 : a_2 : a_3 : b_1 : b_2 : b_3 : b_4)$ corresponds to a polynomial $F = a_1y_2^4 + a_2y_1y_2^2 + a_3y_1^2 + b_1y_1^2y_2 + b_2y_1y_2^3 + b_3y_2^5 + b_4y_1^3$. The algorithm for $MGC(A)$ in Gorenstein colength 2 outputs two ideals:

- $\mathfrak{b} = (b_4) \subset \mathbf{k}[a_1, a_2, a_3, b_1, b_2, b_3, b_4]$;
- $\mathfrak{a} = \left(b_2^2 - b_1b_3\right) \subset \mathbf{k}[a_1, a_2, a_3, b_1, b_2, b_3, b_4]$.

The closed subset $V_+(\mathfrak{b}) \subset \mathbb{P}^6_{\mathbf{k}}$ corresponds to the set of polynomials $F \in \int_{\mathfrak{m}^2} I^\perp/I^\perp$ such that

$$(L_1, \dots, L_{n-1}, L_n^2) \circ F \subseteq I^\perp.$$

Then, $MGC(A) \subset V_+(\mathfrak{b}) = \mathbb{P}^5_{\mathbf{k}}$ and a closed point $p = (a_1 : a_2 : a_3 : b_1 : b_2 : b_3)$ corresponds to a polynomial $F = a_1y_2^4 + a_2y_1y_2^2 + a_3y_1^2 + b_1y_1^2y_2 + b_2y_1y_2^3 + b_3y_2^5$. Finally, $V_+(\mathfrak{a})$ is the closed subset of $\mathbb{P}^5_{\mathbf{k}}$ formed by all non covers of A. Therefore,

$$MCG(A) = \mathbb{P}^5_{\mathbf{k}} \backslash V_+(\mathfrak{a})$$

and $K_F = (x_1, x_2^2)$.

Remark 2.7. Note that the previous constructions strongly depend on the explicit description of the ideal $K_F = (I^\perp :_R F)$. If $\operatorname{gcl}(A) \geq 3$, K_F is no longer unique up to isomorphism, see [8]. According to this paper, if $\operatorname{gcl}(A) \leq 6$ and $\mathbf{k}$ is algebraically closed, there are finitely many isomorphism classes of K_F but they are infinite for $\operatorname{gcl}(A) > 6$. Therefore, although in low cases a similar approach could used to compute $MGC(A)$, there is no direct generalization to any arbitrary Gorenstein colength.

References

[1] H. Ananthnarayan, *The Gorenstein colength of an Artinian local ring*, J. Algebra **320** (2008), no. 9, 3438–3446.

[2] ———, *Computing Gorenstein colength*, J. Commut. Algebra **1** (2009), no. 3, 343–359.

[3] W. Decker, G.-M. Greuel, G. Pfister, and H. Schönemann, SINGULAR *4-0-1 –A computer algebra system for polynomial computations*, www.singular.uni-kl.de, 2014.

[4] J. Elias, INVERSE-SYST.LIB–*Singular library for computing Macaulay's inverse systems*, http://www.ub.edu/C3A/elias/inverse-syst-v.5.2.lib, arXiv:1501.01786, 2015.

[5] J. Elias and R. Homs, *On low Gorenstein colength*, preprint.

[6] J Elias and M. Silva-Takatuji, *On Teter rings*, Proc. Royal Soc. Edim. **147 A** (2017), no. 1, 125–139.

[7] B. Mourrain, *Isolated points, duality and residues*, J. of Pure and Applied Algebra, Elsevier, **117-118** (1996), 469–493.

[8] B. Poonen, *Isomorphism types of commutative algebras of finite rank over an algebraically closed field*, Computational arithmetic geometry, Contemp. Math., vol. 463, Amer. Math. Soc., Providence, RI, 2008, pp. 111–120.

Universitat de Barcelona
E-mail address: elias@ub.edu

Universitat de Barcelona
E-mail address: rhomspon7@ub.edu

Monografías de la Real Academia de Ciencias. Zaragoza. **43:** 87–90, (2018).
ISSN: 1132-6360

FROBENIUS ALGEBRAS OF STANLEY-REISNER RINGS AND MAXIMAL FREE PAIRS

ALBERTO F. BOIX AND SANTIAGO ZARZUELA

Abstract. It is known that the Frobenius algebra of the injective hull of the residue field of a formal power series ring modulo a squarefree monomial ideal can be only principally generated or infinitely generated as algebra over its degree zero piece, and that this fact can be read off in the corresponding simplicial complex; in the infinite case, we exhibit a 1–1 correspondence between potential new generators appearing on each graded piece and certain pairs of faces of such a simplicial complex, that we call maximal free pairs.

Introduction

Let Δ be a simplicial complex with n vertices, we say that a pair (F, G) of non–empty, disjoint faces of Δ is **free** provided $F \cup G$ is the intersection of all the facets containing F. Moreover, given two free pairs $(F, G), (F', G')$, we say that $(F, G) \leq (F', G')$ if $F \supseteq F'$ and $G \subseteq G'$; with this partial order, the set of all the free pairs becomes a partially ordered set. In this way, a free pair (F, G) is said to be **maximal** if it is maximal in the set of free pairs with this order relation.

On the other hand, let K be a field, let $I \subseteq K[x_1, \ldots, x_n] = R$ be the squarefree monomial ideal attached to Δ through the Stanley correspondence, and denote by $I^{[2]}$ the ideal obtained after raising to the square all the elements of I; finally, denote by J_1 the smallest ideal of R containing the set $(I^{[2]} :_R I) \setminus (I^{[2]} + (x_1 \cdots x_n))$.

Keeping in mind all the above notations, the main result of this paper (see Theorem 1.1) is the below:

Theorem 0.1. *There is a 1–1 correspondence between the set of minimal monomial generators of J_1 and the set of maximal free pairs of Δ; in particular, the number of maximal free pairs of Δ coincides with the number of minimal monomial generators for J_1.*

Our motivation to obtain this result comes from [ÀMBZ12], where the authors focused on the so–called Frobenius algebras of Stanley–Reisner rings; for the convenience of the reader, in what follows we review some information about these algebras.

Let A be a commutative Noetherian ring of prime characteristic p and let M be an A–module; given any integer $e \geq 1$, we say that a map $M \xrightarrow{\phi} M$ is *p^e-linear* if, for any $a \in A$

Date: June 30, 2018.
2010 *Mathematics Subject Classification.* Primary 13A35; Secondary 13F55.
Key words and phrases. Frobenius algebras, Stanley–Reisner rings, simplicial complexes, free faces.
A.F.B. is supported by Israel Science Foundation (grant No. 844/14) and Spanish Ministerio de Economía y Competitividad MTM2016-7881-P. S.Z. is supported by Spanish Ministerio de Economía y Competitividad MTM2016-7881-P.

and $m \in M$, $\phi(am) = a^{p^e}\phi(m)$. Since the composition of a p^e-linear map with a $p^{e'}$-linear map produces a $p^{e+e'}$-linear map, one can cook up the algebra

$$\mathcal{F}^M := \bigoplus_{e\geq 0} \mathrm{End}_{p^e}(M),$$

where $\mathrm{End}_{p^e}(M)$ denotes the abelian group made up by all the p^e-linear maps on M; the reader will easily note that $\mathcal{F}^M$ is an associative, positively $\mathbb{N}$–graded, non–commutative ring, and that its degree 1 piece is $\mathrm{End}_A(M)$. $\mathcal{F}^M$ is the so–called *algebra of Frobenius operators* of M. Building upon a counterexample due to Katzman [Kat10], originally motivated by a question raised by Lyubeznik and Smith in [LS01], in [ÀMBZ12] the authors studied $\mathcal{F}^{E_A}$, where $A := K[\![x_1, \ldots, x_n]\!]/I$, K is any field of prime characteristic p, I is a squarefree monomial ideal, and E_A denotes the injective hull of K as A-module; more precisely, it was proved in [ÀMBZ12, Theorem 3.5 and Remarks 3.1.2] that $\mathcal{F}^{E_A}$ is principally generated as A–algebra if and only if $(I^{[2]} : I) = I^{[2]} + (x_1 \cdots x_n)$, otherwise it is infinitely generated as A–algebra. One question not answered in [ÀMBZ12] was whether it is possible to read off the principal (respectively, the infinite) generation of $\mathcal{F}^{E_A}$ in the simplicial complex Δ associated to I through the Stanley correspondence; this question was answered in [ÀMY14], where Àlvarez Montaner and Yanagawa show that, if $\Delta = \mathrm{core}(\Delta)$, then $\mathcal{F}^{E_A}$ is principally generated if and only if Δ does not have free faces (equivalently, if and only if any proper face is contained in at least two facets).

Hereafter, suppose that $\Delta = \mathrm{core}(\Delta)$, and that $\mathcal{F}^{E_A}$ is infinitely generated as A–algebra; on the one hand, by [ÀMBZ12, Theorem 3.5], one knows that $\mathcal{F}^{E_A}$ is infinitely generated if and only if $(I^{[2]} : I) = I^{[2]} + J_1 + (x_1 \cdots x_n)$, where $0 \neq J_1 \not\subseteq I^{[2]} + (x_1 \cdots x_n)$ is the smallest monomial ideal containing the set $(I^{[2]} : I) \setminus I^{[2]} + (x_1 \cdots x_n)$. On the other hand, by [ÀMY14] $\mathcal{F}^{E_A}$ is infinitely generated if and only if Δ has at least one free face. Keeping in mind these two characterizations, one can ask the following:

Question 0.2. *Is there some kind of relation between the number of minimal monomial generators of J_1 and the number of free faces of Δ?*

As we will see, such a relation exists but not directly with the free faces of Δ, instead with maximal free pairs, whereas it is easy to see that free faces are minimal elements of this finite poset. In fact, the correspondence given in Theorem 0.1 is explicit and one can easily extract from the maximal free pairs the corresponding minimal monomial generators of J_1. As application, we use Theorem 0.1 to show (see Theorem 2.1) that, when $\mathcal{F}^{E_A}$ is infinitely generated as A–algebra, the number of new generators appearing on each graded piece is always less or equal than the number of maximal free pairs of the simplicial complex Δ.

The content of this paper is based on [BZ], where the reader can find all the details.

1. Main result

In what follows, let K be a field, and $R = K[x_1, \ldots, x_n]$; we abbreviate the set $\{1, \ldots, n\}$ writing just $[n]$. Finally, given a monomial $m \in R$ we denote by $\mathrm{supp}(m)$ its support and by $\mathrm{supp}_2(m)$ the set of indices i such that $\deg_{x_i}(m) = 2$; keeping in mind these notations, the main result of this paper (see [BZ, Theorem 2.15] for the proof) is the below:

Theorem 1.1. *On the one hand, given a free pair (F,G) as above, set*

$$A(F,G) := \left(\prod_{i\in F} x_i^2\right)\left(\prod_{i\notin F\cup G} x_i\right).$$

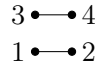
On the other hand, given a monomial $m \in R$ set $Y(m) := (\mathrm{supp}_2(m), [n]\setminus \mathrm{supp}(m))$. Then, the set $\{A(F,G) :\ (F,G)$ maximal free pair of $\Delta\}$ is the minimal monomial generating set for J_1. Moreover, A and Y define $1-1$ correspondences between the set of maximal free pairs of Δ and the set of minimal monomial generators of J_1.

One can turn Theorem 1.1 into a naive algorithm which, receiving any simplicial complex Δ with n vertices as input, returns all its non–empty maximal free pairs in a list L; this method works in the below way.

(i) Compute the corresponding Stanley–Reisner ideal $I \subseteq K[x_1,\ldots,x_n]$, where K is any field.
(ii) Compute $J := (I^{[2]} : I)/(I^{[2]} + (x_1 \ldots x_n))$.
(iii) If $J = 0$, then output that Δ has no free pairs and stop.
(iv) Otherwise, for each minimal monomial generator m of J, add to L the pair (F,G), where $F := \{i \in [n] :\ \deg_{x_i}(m) = 2\}$ and $G := \{i \in [n] :\ \deg_{x_i}(m) = 0\}$.
(v) Output the list L.

We have already implemented this algorithm in Macaulay2 (see [GS13] and [BZ16]); next, we show two examples where we explain, on the one hand, how to use our implementation and how to interpret the output, and, on the other hand, why we really need to consider maximal free pairs, and not just free faces.

Example 1.2. Let Δ be the simplicial complex depicted below:

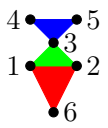


It is easy to see that, for each vertex, there is exactly a maximal free pair and these are all. We check this by using our implementation in the below way:

```
clearAll;
load "FreePairs.m2";
R=ZZ/2 [x,y,z,w,Degrees=>entries id_(ZZ^4)];
I=ideal(x*z,x*w,y*z,y*w);
L=freePairs(I);
L
{{{4}, {3}}, {{2}, {1}}, {{1}, {2}}, {{3}, {4}}}
```

Indeed, the Stanley–Reisner ideal is $I := (xz, xw, yz, yw) \subseteq K[x,y,z,w]$, and $(I^{[2]} : I) = I^{[2]} + (x^2zw, xyz^2, xyw^2, y^2zw) + (xyzw)$, this shows that the maximal free pairs (**that are also the free faces**) of Δ are $(\{1\},\{2\})$, $(\{3\},\{4\})$, $(\{4\},\{3\})$ and $(\{2\},\{1\})$.

Example 1.3. Let Δ be the simplicial complex depicted below:



We use our method to determine all the possible maximal free pairs of Δ as follows:

```
clearAll;
load "FreePairs.m2";
R=ZZ/2 [x,y,z,w,a,b,Degrees=>entries id_(ZZ^6)];
I=ideal(x*w,x*a,y*w,y*a,z*b,w*b,a*b);
L=freePairs(I);
L
{{{6}, {1, 2}}, {{5}, {3, 4}}, {{4}, {3, 5}}, {{2}, {1}},
{{1}, {2}}}
```

Notice that, when (F, G) is either $(\{1\}, \{2\})$ or $(\{2\}, \{1\})$, the face $F \cup G$ turns out to be the intersection of facets $\{1, 2, 3\}$ and $\{1, 2, 6\}$, which are the facets containing F.

2. Application to Frobenius algebras of Stanley–Reisner rings

As we explained in the Introduction, we use in [BZ] Theorem 1.1 to prove the following interesting consequence about these algebras; this is the last result of this paper.

Theorem 2.1. *Let K be any field of prime characteristic, let $R := K[\![x_1, \ldots, x_n]\!]$, let $I = I_\Delta \subseteq R$ be a squarefree monomial ideal, let $A := R/I$, and let E_A denote the injective hull of K as A-module. If $\mathcal{F}^{E_A}$ is infinitely generated as A-algebra, then the number of new generators appearing on each graded piece is always less or equal than the number of maximal free pairs of the simplicial complex Δ.*

References

[ÀMBZ12] J. Àlvarez Montaner, A. F. Boix, and S. Zarzuela. Frobenius and Cartier algebras of Stanley-Reisner rings. *J. Algebra*, 358:162–177, 2012. 87, 88

[ÀMY14] J. Àlvarez Montaner and K. Yanagawa. Addendum to "Frobenius and Cartier algebras of Stanley–Reisner rings" [J. Algebra 358 (2012) 162–177]. *J. Algebra*, 414:300–304, 2014. 88

[BZ] A. F. Boix and S. Zarzuela. Frobenius and Cartier algebras of Stanley–Reisner rings (II). Available at https://arxiv.org/pdf/1712.07836.pdf. 88, 90

[BZ16] A. F. Boix and S. Zarzuela. Freepairs.m2: a Macaulay2 package for computing all the maximal free pairs of a simplicial complex. Available at https://www.math.bgu.ac.il/~fernanal/FreePairs.m2, 2016. 89

[GS13] Daniel R. Grayson and Michael E. Stillman. Macaulay2, a software system for research in algebraic geometry. Available at http://www.math.uiuc.edu/Macaulay2/, 2013. 89

[Kat10] M. Katzman. A non-finitely generated algebra of Frobenius maps. *Proc. Amer. Math. Soc.*, 138(7):2381–2383, 2010. 88

[LS01] G. Lyubeznik and K. E. Smith. On the commutation of the test ideal with localization and completion. *Trans. Amer. Math. Soc.*, 353(8):3149–3180 (electronic), 2001. 88

Department of Mathematics, Ben-Gurion University of the Negev, P.O.B. 653 Beer-Sheva 84105, ISRAEL.

E-mail address: fernanal@post.bgu.ac.il

Departament de Matemàtiques i Informàtica, Universitat de Barcelona, Gran Via de les Corts Catalanes 585, Barcelona 08007, SPAIN

E-mail address: szarzuela@ub.edu

Monografías de la Real Academia de Ciencias. Zaragoza. **43:** 91–94, (2018).
ISSN: 1132-6360

BUCKLING ANALYSIS OF A SIMPLE MECHANICAL SYSTEM

ANDRÉ GALLIGO AND BERNARD ROUSSELET

Abstract. We use computer algebra to analyze the stability, and a generalization of classical Euler buckling, for a simple mechanical systems with 2 degrees of freedom. Our initial aim was to model the behavior under uniaxial compression of a polycarbonate honeycomb.

Introduction

The initial motivation of this work was the following experiment. We considered a polycarbonate honeycomb with circular close-packed cells, a widely used material, that was submitted to a in-plane quasi-static uniaxial compression; see [2], [3], [4], [1]. Since the common tangents to the circles of the plane initial configuration form an (abstract) hexagonal net, there are two different natural directions of compression: when the vertical compression axis is either parallel or perpendicular to a tangent. Our (physicist) colleague Jean Rajchenbach observed that, in the first case, the deformation was homogeneous and compressed all the rows; while, in the second case, the deformation localized along few horizontal rows and was reversible. In order to explain this phenomena, we followed the deformations of the intercellular curved triangles made by 3 portions of circles. It turned out that, when the compression was parallel to a tangent, the curved triangle buckled and rotated, see [1].

Figure 1. Compression of a circular honeycomb in a staggered stack

To mathematically understand this phenomena, we developed a "mesoscopic" approximation of our setting by simpler structures, with few degrees of freedom. Then, analyzed it following [5]. It is the subject of this presentation. We will describe the mechanical model and the mathematical minimization problem of an energy function depending on several parameters.

1. Buckling

We consider several simple mechanical systems with increasing complexity. The first one is an oversimplified model: a rigid bar with an hinge and a vertical load P; we denote by K the torsion coefficient of a rotational spring at the hinge (gravity is neglected). The

vertical displacement is $w = l(1 - \cos(\theta))$; the elastic potential energy is $U = \frac{1}{2}K\theta^2$ the total energy $V = U - Pw$ can be expressed with Lagrangian coordinate θ or $x = l\sin(\theta)$. Then a calculation, which in this case can be performed by hand: $V''(0) = K - Pl$, shows a buckling: for small loads the system is stable at x = 0, but when $P > Kl$, $x = 0$ becomes unstable and two other solutions appear and form a pitchfork bifurcation pattern at $\theta_\pm = \pm\sqrt{6(P/K - 1/l)}(1 + O(\theta^2)$; and we can check that $V''(\theta_\pm) > 0$. In order to define and analyze similarly the total energy of more complicated systems, motivated by our application, we have to rely on Computer algebra.

2. A model with two degrees of freedom

The next figure shows a system made of three bars linked with 2 hinges. One bar is linked to a fixed hinge whereas the third one is linked to an hinge which can move horizontally and on which a horizontal load is applied. The system may be described with 3 angles of the bars with respect to the unloaded configuration ϕ_1, ϕ_2, ϕ_3 (linked by a condition); see the figure below. The work of the applied load is Pw; where the horizontal displacements of the hinges are:

$u_0 = 0, u_1 = l_1(1 - \cos(\phi_1))$, $u_2 = l_1(1 - \cos(\phi_1)) + l_3(1 - \cos(\phi_3))$,

$w = l_1(1 - \cos(\phi_1)) + l_2(1 - cos(\phi_2)) + l_3(1 - \cos(\phi_3))$.

The vertical ones are: $x_0 = 0, x_1 = l_1\sin(\phi_1), x_2 = l_2\sin(\phi_2), x_3 = 0$ and we have: $x_2 - x_1 = l_3\sin(\phi_3)$; $\phi_1 = \arcsin(\frac{x_1}{l_1})$, $\phi_2 = \arcsin(\frac{x_2}{l_2})$ and $\phi_3 = \arcsin(\frac{x_2 - x_1}{l_3})$, with the following bounds $-l_1 \le x_1 \le l_1$, $-l_2 \le x_2 \le l_2$, $-l_3 \le x_2 - x_1 \le l_3$.

We assume that torsion springs are active on hinges A_1 and A_2; we denote with θ_1, θ_2 the relative angle of rotation of each bar with respect to its neighbor; $\theta_1(x_1, x_2) = \phi_1(x_1, x_2) - \phi_3(x_1, x_2)$, $\theta_2(x_1, x_2) = \phi_2(x_1, x_2) + \phi_3(x_1, x_2)$.

Assuming the torsion springs to be linear elastic, the strain energy is $\frac{1}{2}(K_1\theta_1^2 + K_2\theta_2^2)$. Then the total energy involving the work of the applied load is

$$V(x_1, x_2) = \frac{1}{2}[K_1(\theta_1(x_1, x_2))^2 + K_2(\theta_2(x_1, x_2))^2] - Pw(x_1, x_2). \tag{1}$$

With this energy, we get the equilibrium equations: $\frac{\partial V}{\partial x_1} = 0$, $\frac{\partial V}{\partial x_2} = 0$.

2.1. **A special case.**

We assume here that $l_1 = l_2 = l_3 = 1$ and that $K1 = K2 = 1$, and the natural limitation $|x_1| < 1, |x_2| < 1, |x_2 - x_1| < 1$. Then by symmetry, we expect that the equilibrium can be reached only if $x_2 = x_1$ or $x_2 = -x_1$. This is verified by a symbolic computation which eliminates P from the equilibrium equations, i.e. the partial derivatives of the energy V :

$$V = 1/2\ (\arcsin(x_1) + \arcsin(-x_2 + x_1))^2 + 1/2\ (\arcsin(x_2) - \arcsin(-x_2 + x_1))^2$$
$$-P\left(3 - \sqrt{1 - x_1{}^2} - \sqrt{1 - x_2{}^2} - \sqrt{1 - x_2{}^2 + 2\,x_2\,x_1 - x_1{}^2}\right).$$

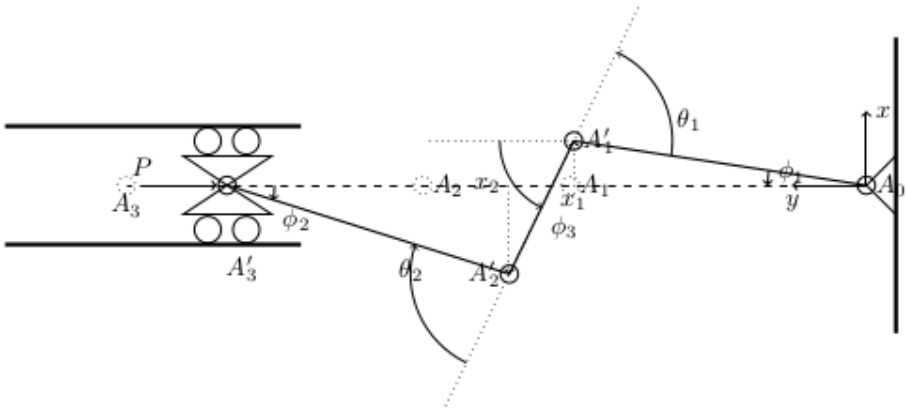
It turns out, after a computation of the Hessian H_V of V that:

For $P < 1$, then $x = 0$ is the only stable equilibrium. For $1 < P < 3$, then $x = 0$ is an unstable equilibrium and two stable (local) equilibriums appears for $x_2 = x_1$ and $P = \frac{\arcsin(x_1)}{x_1}$ i.e $|x_1|$ almost equal to $\sqrt{(6(P-1)}$. For $P > 3$, two stable (local) equilibriums appears for $x_2 = -x_1$ and $|x_1|$ almost equal to $\sqrt{(2(P-3)/3}$. A closer study show that the

corresponding basins of attraction are rather small and that the corresponding value of the total energy V at these points is much higher than its value near the line $x_2 = x_1$.

The first type of buckling is often called a classical Euler buckling, while the second one implies a rotation centered on the center of gravity of the mechanism.

A slight generalization of this case correspond to the symmetric case when $l_1 = l_2$ and that $K1 = K2$. A symbolic computation shows again that there are similarly two types of bucklings, one when $x_2 = x_1$ for $P > P1$ and another one when $x_2 = -x_1$ for $P > P_2 > P_1$; for some values P_1 and P_2 which can be expressed as functions of the parameters. In order to show that these equilibriums are stable, we had to approximate the energy by a Taylor expansion up to order four.



2.2. **Non symmetric case.** To simplify the notations (to avoid some quotients), we let $m_1 = 1/l_1$, $m_2 = 1/l_2$, $m_3 = 1/l_3$. the following computations required a Computer algebra system.

2.2.1. *Second order approximation of energy.*

$$U_2 = \frac{1}{2}\left(K_2 m_3^2 + \left(m_1^2 + 2\,m_1 m_3 + m_3^2\right)K_1\right)x_1^2$$
$$-\left(\left(m_1 m_3 + m_3^2\right)K_1 + \left(m_2 m_3 + m_3^2\right)K_2\right)x_1 x_2$$
$$+\frac{1}{2}\left(K_1 m_3^2 + \left(m_2^2 + 2\,m_2 m_3 + m_3^2\right)K_2\right)x_2^2$$
$$wtaylor = \frac{1}{2}(m_1 + m_3)x_1^2 - m_3 x_1 x_2 + \frac{1}{2}(m_2 + m_3)x_2^2.$$

Hence the Hessian H_V is

$$\begin{pmatrix} K_2 m_3^2 + \left(m_1^2 + 2\,m_1 m_3 + m_3^2\right)K_1 - (m_1 + m_3)P & -\left(m_1 m_3 + m_3^2\right)K_1 - \left(m_2 m_3 + m_3^2\right)K_2 + m_3 P \\ -\left(m_1 m_3 + m_3^2\right)K_1 - \left(m_2 m_3 + m_3^2\right)K_2 + m_3 P & K_1 m_3^2 + \left(m_2^2 + 2\,m_2 m_3 + m_3^2\right)K_2 - (m_2 + m_3)P \end{pmatrix}$$

Then, we can explicitly compute the two eigenvalues λ_1 and λ_2 which will define the bifurcation.

2.2.2. *Buckling load.* When $\lambda_1 = 0$. we obtain two values of P; we use the smallest one P_1 with:

$$P_1 = \frac{1}{2}\,K_1 m_1 + \frac{1}{2}\,K_2 m_2 + \frac{1}{2}\,(K_1 + K_2) m_3 - \frac{1}{2}\,\sqrt{R_p}$$

$$R_p = K_1^2 m_1^2 - 2\,K_1 K_2 m_1 m_2 + K_2^2 m_2^2 + \big(K_1^2 + 2\,K_1 K_2 + K_2^2\big) m_3^2$$

$$+2\,\Big(\big(K_1^2 - K_1 K_2\big) m_1 - \big(K_1 K_2 - K_2^2\big) m_2\Big) m_3, p_+ = \frac{1}{2}\,K_1 m_1 + \frac{1}{2}\,K_2 m_2 + \frac{1}{2}\,(K_1 + K_2) m_3 + \frac{1}{2}\,\sqrt{R_p}$$

$$R_p = K_1^2 m_1^2 - 2\,K_1 K_2 m_1 m_2 + K_2^2 m_2^2 + \big(K_1^2 + 2\,K_1 K_2 + K_2^2\big) m_3^2$$

$$+2\,\Big(\big(K_1^2 - K_1 K_2\big) m_1 - \big(K_1 K_2 - K_2^2\big) m_2\Big) m_3.$$

And we had to check that $P_1 > 0$.

2.2.3. *An example.* We choose $K_1 := 2; K_2 := 1; m_1 := .1; m_2 := .12; m_3 := 1$.

We found that for the loads $P_1 = 0.1461968424, , P_2 = 3.1738031584$, we get two bucklings in the directions tangent to $x_2 = 1.026901579\ x_1$ and to $x_2 = -0.4869015788\ x_1$, which follow behaviors similar to those described for the symmetric case.

References

[1] Galligo, A. and Rajchenbach, J. and Rousselet, B.: Compression of a polycarbonate honeycomb. Preprint Université de Nice, (2018).

[2] Hu, L.L. and Yu, T and Y. Gao, Z and Huang, X.Q.: The inhomogeneous deformation of polycarbonate circular honeycombs under in-plane compression. International Journal of Mechanical Sciences (2008),volume = 50.

[3] López Jiménez, F. and Triantafyllidis, N.: Buckling of rectangular and hexagonal honeycomb under combined axial compression and transverse shear. International Journal of Solids and Structures, 50(24), pp.3934–3946, (2013).

[4] S.D. Papka, S. Kyriakides: In-plane crushing of a polycarbonate honeycomb. Int. J. Solids Struct., 35 (1998), pp. 239–267

[5] Rousselet, B.: A Finite Strain Rod Model and Its Design Sensitivity. Optimization of Large Structural Systems, Springer Netherlands (1993).

André Galligo, LJAD and INRIA, University Cote d'Azur, 06108 Nice, France.
E-mail address: galligo@unice.fr

Bernard Rousselet, LJAD University Cote d'Azur, 06108 Nice, France.
E-mail address: bernard.rousselet@unice.fr

Monografías de la Real Academia de Ciencias. Zaragoza. **43:** 95–98, (2018).
ISSN: 1132-6360

LOWER BOUNDS BY BIRKHOFF INTERPOLATION

IGNACIO GARCÍA-MARCO AND PASCAL KOIRAN

Abstract. In this work we give lower bounds for the representation of real univariate polynomials as sums of powers of degree 1 polynomials. We present two families of polynomials of degree d such that the number of powers that are required in such a representation must be at least of order d. This is clearly optimal up to a constant factor. Previous lower bounds for this problem were only of order $\Omega(\sqrt{d})$, and were obtained from arguments based on Wronskian determinants and "shifted derivatives". We obtain this improvement thanks to a new lower bound method based on Birkhoff interpolation.

In this paper we obtain lower bounds for the representation of a univariate polynomial $f \in \mathbb{R}[x]$ of degree d under the form:

$$f(x) = \sum_{i=1}^{l} \beta_i (x + y_i)^{e_i} \tag{1}$$

where the β_i, y_i are real constants and the exponents e_i nonnegative integers.

We give two families of polynomials such that the number l of terms required in such a representation must be at least of order d. This is clearly optimal up to a constant factor. Previous lower bounds for this problem [6] were only of order $\Omega(\sqrt{d})$. The polynomials in our first family are of the form $H_1(x) = \sum_{i=1}^{k} \alpha_i (x + x_i)^d$ with all α_i nonzero and the x_i's distinct. We show that they require at least $l \geq k$ terms whenever $k \leq (d+2)/4$. In particular, for $k = (d+2)/4$ we obtain $l = k = (d+2)/4$ as a lower bound. The polynomials in our second family are of the form $H_2(x) = (x+1)^{d+1} - x^{d+1}$ and we show that they require more than $(d-1)/2$ terms. This improves the lower bound for H_1 by a factor of 2, but this second lower bound applies only when the exponents e_i are required to be bounded by d (obviously, if larger exponents are allowed we only need two terms to represent H_2). It is easily shown that every polynomial of degree d can be represented with $\lceil (d+1)/2 \rceil$ terms. This implies that of all polynomials of degree d, H_2 is essentially the hardest one.

Our lower bound results are specific to polynomials with real coefficients. It would be interesting to obtain similar lower bounds for other fields, e.g., finite fields or the field of complex numbers.

Motivation and connection to previous work. Lower bounds for the representation of univariate polynomials as sums of powers of *low degree* polynomials were recently obtained in [6]. We continue this line of work by focusing on powers of *degree one* polynomials. This problem is still challenging because the exponents e_i may be different from $d = \deg(f)$, and may be possibly larger than d. The lower bounds obtained in [6] are of order $\Omega(\sqrt{d})$. We obtain $\Omega(d)$ lower bounds with a new method based on polynomial interpolation.

The work in [6] and in the present paper is motivated by recent progress in arithmetic circuit complexity. It was shown that strong enough lower bounds for circuits of depth

four or even depth three [1, 8] would yield a separation of Valiant's [9] algebraic complexity classes VP and VNP. Moreover, lower bounds for such circuits were obtained thanks to the introduction by Neeraj Kayal of the method of *shifted partial derivatives*, see e.g. [5]. Some of these lower bounds seem to come close to separating VP from VNP. Nevertheless, this method cannot prove more than a $1.5m^2$ lower bound on the determinantal complexity of the $m \times m$ permanent [4]. It is therefore desirable to develop new lower bounds methods. We view the models studied in [6] and in the present paper as "test beds" for the development of such methods in a fairly simple setting.

Birkhoff interpolation. As mentioned above, our results are based on polynomial interpolation and more precisely on Birkhoff interpolation (also known as "lacunary interpolation"). In a typical Birkhoff interpolation problem, one may have to find a polynomial g of degree at most 5 satisfying the 4 constraints: $g(0) = 0$, $g'(1) = 0$, $g(2) = g''(2) = 0$. Our interest is in the existence of a nonzero polynomial of degree at most d satisfying the constraints, and more generally in the dimension of the solution space. In fact, we need to know whether it has the dimension that one would expect by naively counting the number of constraints. This is a nontrivial problem and a rich theory was developed to address it [7]. Results of the real (as opposed to complex) theory of Birkhoff interpolation turn out to be very well suited to our lower bound problems. This is the reason why we work with real polynomials.

The Waring problem. Any homogeneous (multivariate) polynomial can be written as a sum of powers of linear forms. In the Waring problem for polynomials one attempts to determine the *Waring rank*, the smallest possible number of powers in such a representation. Obtaining lower bounds from results in polynomial interpolation seems to be a new method in complexity theory, but it may not come as a surprise to experts on the Waring problem. Indeed, a major result in this area, the Alexander-Hirschowitz theorem ([2]), is usually stated as a result on polynomial interpolation. We expect that more connections between lower bounds in algebraic complexity and polynomial interpolation will be uncovered.

1. From linear independence to polynomial interpolation

There is a clear connection between lower bounds for representations of polynomials under form (1) and linear independence. Indeed, proving a lower bound for a polynomial f amounts to showing that f is linearly independent from $(x + y_1)^{e_1}, \ldots, (x + y_l)^{e_l}$ for some l and for any sequence of l pairs $(y_1, e_1), \ldots, (y_l, e_l)$. This motivates our study.

Let $\mathbb{R}_d[x]$ denote the linear subspace of $\mathbb{R}[x]$ made of polynomials of degree at most d, and by $g^{(k)}$ th k-th order derivative of a polynomial g.

Proposition 1.1. *Let $f_1, \ldots, f_k \in \mathbb{R}_d[x]$ be k distinct polynomials of the form $f_i(x) = (x + a_i)^{e_i}$. The family $(f_i)_{1 \leq i \leq k}$ is linearly independent if and only if*

$$\dim\{g \in \mathbb{R}_d[x];\ g^{(d-e_i)}(a_i) = 0 \text{ for all } i\} = d + 1 - k.$$

2. Interpolation matrices

In Birkhoff interpolation we look for a polynomial $g \in \mathbb{R}_d[x]$ satisfying a system of equations of the form

$$g^{(k)}(x_i) = c_{i,k},\ \textit{where } x_i, c_{i,k} \in \mathbb{R} \textit{ and } k \leq d. \tag{2}$$

We set $e_{i,k} = 1$ if such an equation appears, and $e_{i,k} = 0$ otherwise. We arrange this combinatorial data in an *interpolation matrix* $E = (e_{i,k})_{1\le i\le m, 0\le k\le d}$ of size $m \times (d+1)$. We assume that the *knots* $x_1, \dots, x_m$ are distinct. It is usually assumed [7] that the number of 1's in E, denoted by $|E|$ is equal to $d+1$. Here we will only assume that $|E| \le d+1$.

Let $X = \{x_1, \dots, x_m\}$ be the set of knots. When $|E| = d+1$, the pair (E, X) is said to be *regular* if (2) has a unique solution for any choice of the $c_{i,k}$. Finding necessary or sufficient conditions for regularity has been a major topic in Birkhoff interpolation [7]. For $|E| \le d+1$, we may expect (2) to have a set of solutions of dimension $d+1-|E|$.

Definition 2.1. The pair (E, X) is regular if for any choice of the $c_{i,k}$ the set of solutions of (2) is an affine subspace of dimension $d+1-|E|$. The interpolation matrix E is regular if (E, X) is regular for any choice of m knots $x_1, \dots, x_m$.

We will give in Theorem 2.2 a sufficient condition for regularity, but we first need some additional definitions. Say that an interpolation matrix E satisfies the *Pólya condition* if for $r = 1, \dots, d+1$ there are at most r 1's in the last r columns of E.

Consider a row of an interpolation matrix E. By *sequence* we mean a maximal sequence of consecutive 1's in this row. A sequence containing an odd number of 1's is naturally called an *odd sequence*.

The following result is a particular case of an important result due to Atkinson and Sharma [3].

Theorem 2.2. *Let E be an interpolation matrix with $|E| = d+1$. If E satisfies the Pólya condition and all odd sequences begin in the first column, then E is regular.*

We use this result to prove the main result of this section.

Theorem 2.3. *Let E be an interpolation matrix. We denote by N_r the number of 1's in the last r columns of E. If $N_1 \le 1$ and $N_r + N_{r-1} \le r$ for $r = 2, \dots, d+1$ then E is regular.*

Putting together Proposition 1.1 and Theorem 2.3, we get a result on the linear independence of polynomials which may be of independent interest.

Theorem 2.4. *Let $f_1, \dots, f_k \in \mathbb{R}[x]$ be k distinct polynomials of the form $f_i(x) = (x+a_i)^{e_i}$. Let us denote by n_j the number of polynomials of degree less than j in this family.*

If $n_1 \le 1$ and $n_j + n_{j-1} \le j$ for all j, the family (f_i) is linearly independent.

3. Lower bounds

In this section we apply the previous results to derive the desired lower bounds.

Theorem 3.1 (First lower bound)**.** *Consider a polynomial of the form*

$$H_1(x) = \sum_{i=1}^{k} \alpha_i (x + x_i)^d \tag{3}$$

where the x_i are distinct real constants, the α_i are nonzero real constants, and $k \le (d+2)/4$. If H_1 is written as $H_1(x) = \sum_{i=1}^{l} \beta_i (x + y_i)^{e_i}$, then we must have $l \ge k$.

In other words, writing H_1 under form (3) is optimal when $k \le (d+2)/4$. We give another lower bound of order d (with an improved constant) for a polynomial of a different form.

Theorem 3.2 (Second lower bound)**.** *Let $H_2 \in \mathbb{R}_d[x]$ be the polynomial $H_2(x) = (x+1)^{d+1} - x^{d+1}$. If H_2 is written under the form $H_2(x) = \sum_{i=1}^{l} \beta_i (x+y_i)^{e_i}$, with $e_i \leq d$ for every i then we must have $l > (d-1)/2$.*

This result shows that allowing exponents $e_i > d$ can drastically decrease the "complexity" of a polynomial since H_2 can be expressed as the difference of only two $(d+1)$-st powers.

4. Lower bounds over the complex numbers

Some of the proof techniques and the results of this work are specific to the field of real numbers. This is due to the fact that certain linear dependence relations which cannot occur over $\mathbb{R}$ may occur over $\mathbb{C}$. We begin with an identity over the complex.

Proposition 4.1. *Take $k \in \mathbb{Z}^+$ and let ξ be a k-th primitive root of unity. Then, for all $d \in \mathbb{Z}^+$ and all $\mu \in \mathbb{C}$ the following equality holds:*

$$\sum_{j=1}^{k} \xi^j (x + \xi^j \mu)^d = \sum_{\substack{i \equiv -1 \pmod{k} \\ 0 \leq i \leq d}} k \binom{d}{i} \mu^i x^{d-i}.$$

As a consequence of this identity, one can prove that no better lower bound than $\Omega(\sqrt{d})$ can possibly hold over $\mathbb{C}$ for the family of polynomials of Theorem 3.1, at least for arbitrary distinct x_i's and arbitrary nonzero α_i. We leave it as an open problem to close this quadratic gap between lower bounds over $\mathbb{R}$ and $\mathbb{C}$. With the additional requirements $e_i \leq d$ for all i, the polynomial $H_2(x) = (x+1)^{d+1} - x^{d+1}$ from Theorem 3.2 looks like a plausible candidate.

References

[1] M. Agrawal and V. Vinay. Arithmetic circuits: A chasm at depth four. In *Proc. 49th IEEE Symposium on Foundations of Computer Science*, pages 67–75, 2008.

[2] J. Alexander and A. Hirschowitz. Polynomial interpolation in several variables. *Journal of Algebraic Geometry*, 4(2):201–222, 1995.

[3] K. Atkinson and A. Sharma. A partial characterization of poised Hermite-Birkhoff interpolation problems. *SIAM Journal on Numerical Analysis*, 6(2):230–235, 1969.

[4] K. Efremenko, J. M. Landsberg, H. Schenck and J. Weyman. The method of shifted partial derivatives cannot separate the permanent from the determinant *arXiv preprint arXiv:1609.02103 [math.AG]*, 2016.

[5] N. Kayal. An exponential lower bound for the sum of powers of bounded degree polynomials. *Electronic Colloquium on Computational Complexity (ECCC)*, 19, 2012.

[6] N. Kayal, P. Koiran, T. Pecatte and C. Saha. Lower bounds for sums of powers of low degree univariates. In *Proc. ICALP 2015, part I*, LNCS 9134, pages 810–821. Springer, 2015.

[7] G. G. Lorentz, K. Jetter, and S. D. Riemenschneider. *Birkhoff interpolation*, volume 19 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, 1984.

[8] S. Tavenas. Improved bounds for reduction to depth 4 and depth 3. In *Proc. 38th International Symposium on Mathematical Foundations of Computer Science (MFCS)*, 2013.

[9] L. G. Valiant. Completeness classes in algebra. In *Proc. 11th ACM Symposium on Theory of Computing*, pages 249–261, 1979.

Facultad de Ciencias, Sección de Matemáticas, Universidad de La Laguna. Spain
E-mail address: iggarcia@ull.es

LIP, ENS Lyon - CNRS - UCBL - INRIA, Université de Lyon UMR 5668, Lyon, France
E-mail address: pascal.koiran@ens-lyon.fr

Monografías de la Real Academia de Ciencias. Zaragoza. **43:** 99–102, (2018).
ISSN: 1132-6360

CÁLCULO APROXIMADO DE LA DISTANCIA MÍNIMA DE UN CÓDIGO LINEAL

JOSÉ GÓMEZ-TORRECILLAS, F. J. LOBILLO Y GABRIEL NAVARRO

Resumen. Mostramos una aplicación de los algoritmos aproximados al problema NP-duro del cálculo de la distancia mínima de un código lineal sobre un cuerpo finito. En particular, desarrollamos un algoritmo genético para obtener una cota superior. A diferencia de los algoritmos (exactos o aproximados) presentes en la literatura, la eficiencia teórica no es polinómica solamente respecto de la longitud del código.

Introducción

A la hora de valorar la utilidad práctica de un código lineal, la distancia mínima es uno de los parámetros principales, ya que permite calcular la capacidad de corrección de dicho código. Entre los algoritmos desarrollados para su cálculo, el más rápido es el algoritmo de Brouwer-Zimmermann (BZ), ver [2]. Aunque el algoritmo de BZ puede aplicarse a códigos sobre cualquier cuerpo finito, en la práctica sólo puede ser considerado eficaz para códigos binarios. Sin embargo, existen situaciones donde es necesario trabajar sobre códigos no binarios. Por ejemplo, en el diseño de códigos cíclicos torcidos [5], tanto de bloque como convolucionales, y sus algoritmos de decodificación [6, 8] se necesita que el cuerpo finito base tenga un cardinal relativamente grande (ver los ejemplos de [7]). Esto es así puesto que, a mayor longitud, es necesario aumentar el cardinal del cuerpo.

Es conocido que el cálculo de la distancia es un problema NP-duro, y su problema de decisión asociado, NP-completo [10]. Así, salvo que P=NP, no puede existir un algoritmo (exacto) que calcule la distancia de cualquier código lineal en un tiempo razonable. Aunque en la literatura pueden encontrarse algoritmos aproximados, como, por ejemplo, en [1] o en [9], todos estos métodos siguen considerando un espacio de soluciones que crece de forma exponencial respecto al cardinal del subcuerpo primo así como respecto de la dimensión del código. Nuestra propuesta consiste en el diseño, e implementación, de un algoritmo aproximado cuyo espacio de de soluciones y tiempo de ejecución únicamente depende no polinomialmente de la longitud del código. Concretamente, diseñamos un algoritmo genético, basado en un modelo generacional clásico, para el cálculo de una cota superior de la distancia.

1. Algoritmo genético GLN

Los *algoritmos genéticos* son un tipo de metaheurísticas que siguen un modelo de búsqueda basado en poblaciones consistente en simular el proceso de combinación genética. Consultar [4, Capítulo 3] para una referencia básica. A continuación detallamos los módulos que componen el Algoritmo 2.

1.1. Representación del espacio de búsqueda. El desarrollo de un algoritmo genético requiere, en primer lugar, representar el espacio de soluciones del problema mediante cierta codificación (los *cromosomas*) de manera que, por *recombinación* de ellos y *mutación*, nos aproximemos a algún cromosoma óptimo. Para el problema de la distancia mínima, una representación obvia es considerar una extensión de la utilizada en [1] para códigos binarios, de modo que el espacio de soluciones sea un $\mathbb{F}_q$–espacio vectorial de dimensión k. Sin embargo, con esta representación, el tamaño de dicho espacio aumenta de forma exponencial respecto del tamaño del subcuerpo primo (así como de k). Nuestra propuesta considera un espacio de representación que no depende del cuerpo. Para ello, necesitamos el siguiente resultado. Aunque su demostración no es complicada, no lo hemos encontrado en la literatura.

Teorema 1.1. *Sea G una matriz $k \times n$ generadora de un código $[n,k]$-lineal $\mathcal{C}$ sobre el cuerpo finito $\mathbb{F}_q$. Existe una permutación $P \in \mathcal{S}_n$ tal que la matriz reducida por filas R de GM_P, donde M_P es la matriz asociada a P, verifica que el peso de Hamming de alguna de sus filas coincide con la distancia mínima de $\mathcal{C}$. Además, si b es la fila de R verificando tal propiedad, entonces bM_P^{-1} es una palabra de $\mathcal{C}$ de peso mínimo.*

Por tanto, el problema de calcular la distancia mínima de un código lineal se reduce a calcular el mínimo de la aplicación $\mathfrak{d} : \mathcal{S}_n \to \mathbb{N}$ definida como

$$\mathfrak{d}(P) = \text{mín}\{\text{w}(b) \,|\, b \text{ es una fila de la matriz reducida por filas de } GM_P\},$$

donde $\text{w}(b)$ denota el peso de Hamming del vector b. Nótese que con esta representación el espacio de soluciones sólo depende de la longitud del código. En particular, es invariante respecto al tamaño del cuerpo. Obviamente, el cálculo de la imagen de una permutación por $\mathfrak{d}$ sí depende del cuerpo y de la dimensión del código. Sin embargo, la eficiencia de este cálculo respecto del cuerpo primo y la dimensión es polinomial.

1.2. Operador de cruce. La recombinación de cromosomas es uno de los puntos clave para conseguir un equilibrio adecuado entre *diversidad* (exploración de diferentes zonas del espacio de búsqueda) y *convergencia* en el comportamiento del algoritmo. Los operadores de cruce clásicos no consideran la estructura algebraica del grupo $\mathcal{S}_n$. En esta comunicación proponemos basar el operador de cruce en el producto de permutaciones, ya que dos (o más) elementos al azar de $\mathcal{S}_n$ probablemente formen un sistema de generadores (Teorema de Dickson [3, Theorem 1]) y, por tanto, podemos esperar una diversidad suficiente para obtener un cromosoma óptimo. Concretamente, definimos una familia de cruces algebraicos AX_r, donde r es el número de cromosomas involucrados. Para r cromosomas $p_1, p_2, \ldots, p_r$ consideramos

$$\mathcal{T} = \{p_{\tau(1)} \circ p_{\tau(2)} \circ \cdots \circ p_{\tau(r)} \text{ tal que } \tau \in \mathcal{S}_r\}.$$

De esta familia seleccionamos los r cromosomas con menor imagen por $\mathfrak{d}$ (aquellos que presentan una mejor adaptación) que reemplazarán a los cromosomas originales. Mantendremos ciertos conjuntos de individuos sin cruce utilizando una probabilidad de cruce p_c. En la Sección 2, utilizaremos $p_c = 0{,}7$, que es el valor más común en la literatura.

1.3. Operador de mutación. Este operador aumenta la diversidad al permitir la mutación de algunos genes (componentes de un cromosoma). El operador de mutación estándar consiste en la multiplicación por una transposición aleatoria. Sin embargo, en este problema,

la mutación por una transposición no suele cambiar el valor de $\mathfrak{d}$, por lo que utilizaremos ciclos de longitud $\lfloor n/2 \rfloor$. La probabilidad de mutación utilizada en la Sección 2 es $p_m = 0{,}1$.

1.4. Relevo generacional. Con las características anteriores, podemos diseñar el Algoritmo 1 para el cálculo de una población a partir otra existente. Está basado en un modelo generacional básico: la nueva población reemplaza a la antigua. Para aumentar la convergencia, la población resultante hereda el cromosoma con mejor adaptación (esto recibe el nombre de elitismo).

Algoritmo 1 RelevoGeneracional

Entrada: $P(i)$, población en el instante $i \geq 0$; G, matriz generadora; p_c, probabilidad de cruce; p_m, probabilidad de mutación; r, cardinal del conjunto susceptible de cruzarse.
Salida: $P(i+1)$ población en el instante $i+1$.

$best \leftarrow$ cromosoma donde se alcanza el mínimo de $\mathfrak{d}$ para $P(i)$.
$X \leftarrow \emptyset$
Mientras $\#P(i) \geq r$ **hacer**
  $\mathcal{S} \leftarrow \{r$ cromosomas elegidos aleatoriamente de $P(i)\}$.
  $P(i) \leftarrow P(i) - \mathcal{S}$
  $\mathcal{S} \leftarrow \begin{cases} AX_r(\mathcal{S}) \text{ con probabilidad } p_c, \\ \mathcal{S} \text{ con probabilidad } 1 - p_c. \end{cases}$
  Para $s \in \mathcal{S}$ **hacer**
    $s \leftarrow \begin{cases} s \circ p \text{ con probabilidad } p_m,\ p \text{ ciclo aleatorio de longitud } \lfloor n/2 \rfloor \\ s \text{ con probabilidad } 1 - p_m. \end{cases}$
  $X \leftarrow X \cup \mathcal{S}$
Devolver $X \cup \{best\}$

1.5. Población inicial. Como población inicial utilizaremos $2n$ permutaciones elegidas aleatoriamente. Puesto que cualquier permutación se obtiene como un producto de los elementos de un sistema de generadores, buscamos que la población activa probablemente forme un sistema de generadores de $\mathcal{S}_n$. El Algoritmo 2 recoge todos los módulos explicados en esta sección.

Algoritmo 2 Algoritmo genético GLN

Entrada: (G, r, p_m, p_c), como en Algoritmo 1; c ó t, número máximo de iteraciones ó tiempo máximo de ejecución, respectivamente.
Salida: $\overline{d}$ cota superior de la distancia mínima de $\mathcal{C}$.

$P(0) \leftarrow$ Población inicial aleatoria de tamaño $2n$.
$i \leftarrow 1$
Mientras $i < c$ (ó $time < t$) **hacer**
  $P(i) \leftarrow$ RelevoGeneracional$(P(i-1), G, r, p_c, p_m)$
  $i \leftarrow i + 1$
$best \leftarrow$ cromosoma donde se alcanza el mínimo de $\mathfrak{d}$ para $P(i)$.
Devolver $\mathfrak{d}(best)$

2. Resultados experimentales

En el Cuadro 1 mostramos los resultados experimentales preliminares al aplicar el Algoritmo 2 a algunos de los códigos lineales de la base de datos de `http://codetables.de`. Las matrices generadoras correspondientes han sido calculadas con MAGMA usando la función BKLC. El Algoritmo 2 ha sido implementado en Sagemath (Python). La ejecución del algoritmo se ha realizado usando un procesador Intel Core i7 3GHz bajo el sistema operativo macOS 10.12.6. Como comparación, una implementación del algoritmo de BZ requiere un tiempo de ejecución estimado de más de 40 horas para el código $[30, 12, 14]_8$-lineal

n	k	d	tiempo medio (seg.)	n	k	d	tiempo medio (seg.)
30	12	14	0.15	60	25	24	0.38
30	14	12	0.16	60	33	18	0.40
30	16	10	0.16	60	41	12	0.43
45	18	19	0.26	75	25	33	5.43
45	21	16	0.69	75	35	24	3.31
45	25	13	0.27	75	45	17	10.15

Cuadro 1. Tiempo medio (100 repeticiones del Algoritmo 2 con AX_2) para alcanzar la distancia mínima en algunos códigos $[n, k, d]$-lineales sobre $\mathbb{F}_8$

Investigación financiada por la ayuda MTM2016-78364-P de la Agencia Estatal de Investigación y FEDER.

Referencias

[1] M. Askali, A. Azouaoui, S. Nouh, M. Belkasmi. On the computing of the minimum distance of linear block codes by heuristic methods, International Journal of Communications, Network and System Sciences 5 (11) (2012), 774–784.
[2] A. Betten, M. Braun, H. Fripertinger, A. Kerber, A. Kohnert, A. Wassermann. Error-Correcting Linear Codes. Algorithms and Computation in Mathematics 18. Springer. 2006.
[3] J. D. Dixon, The probability of generating the symmetric group. Mathematische Zeitschrift, 110 (1969), 199–205.
[4] E-G. Talbi. Metaheuristics: From Design to Implementation. John Wiley & Sons, Inc. 2009.
[5] J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro. A new perspective of cyclicity in convolutional codes, IEEE Transactions on Information Theory 62 (5) (2016), 2702–2706.
[6] J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro. A Sugiyama-like decoding algorithm for convolutional codes, IEEE Transactions on Information Theory 63 (2017) 6216–6226.
[7] J. Gómez-Torrecillas, F.J. Lobillo G. Navarro A. Neri. Hartmann-Tzeng bound and skew cyclic codes of designed Hamming distance, Finite Fields and Their Applications 50 (2018), 84–112.
[8] J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro. Peterson-Gorenstein-Zierler algorithm for skew RS codes, Linear and Multilinear Algebra 66 (2018), 469–487.
[9] J. S. Leon. A probabilistic algorithm for computing minimum weights of large error-correcting codes, IEEE Transactions on Information Theory 34 (5) (1988), 1354–1359.
[10] A. Vardy. The intractability of computing the minimum distance of a code, IEEE Transactions on Information Theory 43 (6) (1997), 1757–1766.

Departamento de Álgebra y CITIC, Universidad de Granada
E-mail address: `gomezj@ugr.es`
E-mail address: `jlobillo@ugr.es`

Departamento de Ciencias de la Computación e IA y CITIC, Universidad de Granada
E-mail address: `gnavarro@ugr.es`

Monografías de la Real Academia de Ciencias. Zaragoza. **43:** 103–106, (2018).
ISSN: 1132-6360

AN EFFECTIVE STUDY OF SERRE SPECTRAL SYSTEMS

ANDREA GUIDOLIN AND ANA ROMERO

Abstract. In this paper we use the technique of effective homology to compute spectral systems, a generalization of classical spectral sequences which are defined for filtrations indexed over any partially ordered set (poset). In particular, we focus our study on the Serre spectral system associated with a tower of fibrations, showing some considerations on the different levels of this spectral system and computing some results by means of a new module for the Kenzo computer algebra system.

Introduction

The notion of spectral sequence has been recently generalized by Benjamin Matschke [Mat13] to a much broader perspective. The most innovative aspect of his remarkable construction is that it applies to filtrations of chain complexes indexed over any partially ordered set (poset), rather than being limited to filtrations indexed over the set $\mathbb{Z}$ of integer numbers as for classical spectral sequences. The collection of groups produced by his generalized construction, which he calls a *spectral system*, is larger than in the classical scenario, as more parameters are taken into account. In addition to giving a formal definition and some general results about spectral systems, the paper [Mat13] includes several interesting particular cases which generalize the classical spectral sequences of Serre, Eilenberg-Moore and Adams-Novikov. However, as in the case of spectral sequences associated with a linear filtration, no algorithm is provided computing the different components when the initial spaces are not of finite type.

In this work we present a study of spectral systems, using the technique of *effective homology* [RS02] to produce algorithms and programs for computing spectral systems of chain complexes of infinite type. In particular we focus on the Serre spectral system of a tower of fibrations, an interesting example of spectral system associated with a filtration over $D(\mathbb{Z}^m)$, the poset of downsets of $\mathbb{Z}^m$.

1. Spectral systems over a poset

The following definitions can be found in [Mat13].

Definition 1.1. A filtration of a chain complex C_* over a poset $(I, \leq)$, briefly called an I-filtration, is a collection of subcomplexes $F = (F_i C_*)_{i \in I}$ such that

$$i \leq j \text{ in } I \quad \Longrightarrow \quad F_i C_* \subseteq F_j C_*.$$

The second author has been partially supported by Ministerio de Economía, Industria y Competitividad, Spain, project MTM2017-88804-P.

We will denote the chain subcomplexes simply as F_i, forgetting about the grading of homology, when we are only interested in the filtration index i.

Definition 1.2. Let (C_*, F) be an I-filtered chain complex. Given a 4-tuple of indices $z \leq s \leq p \leq b$ in I we define

$$S[z,s,p,b] = \frac{F_p \cap d^{-1}(F_z)}{d(F_b) + F_s}, \tag{1}$$

where by convention the quotient A/B of abelian groups on the right member denotes the quotient $A/(B \cap A)$. We call the collection $(S[z,s,p,b])_{z \leq s \leq p \leq b}$ the *spectral system* associated with the I-filtration $F = (F_i)_{i \in I}$ of C_*, and we call each abelian group $S[z,s,p,b]$ a *term* of the spectral system.

This definition generalizes that of a spectral sequence associated with a linear filtration (see for example [Mac63]). Moreover, as in the classical scenario, a notion of *page* of a spectral system can be defined (based on the choice of the 4-tuples of indices z, s, p, b), as well as differential maps which allow to obtain the next page of a given one by taking homology (see [Mat13] for details).

Although some interesting examples of generalized spectral sequences associated with *interesting* objects are defined (for example, the generalized Serre spectral system explained in Section 3), all the definitions in [Mat13] are formal and the paper does not include a method for computing the spectral systems. In particular, the formula (1) can only be determined in some simple situations (when the chain complex C_* is of finite type).

2. Effective homology for computing spectral systems

In order compute spectral systems, in a previous work [GR18] we used the method of effective homology [RS02] to produce algorithms computing spectral systems of complicated filtered chain complexes, even when they are of infinite type. Our programs were implemented in the system Kenzo [DRSS99], and work in a similar way to the method that this symbolic computation system uses to determine homology groups of a given chain complex: if an I-filtered complex C_* is of finite type, its spectral system can be determined by means of diagonalization algorithms on some matrices. Otherwise, a pair of *reductions* $C_* \twoheadleftarrow \hat{C}_* \twoheadrightarrow D_*$ from the initial chain complex C_* to another one D_* of finite type (also filtered over I) is constructed. The chain complex D_* is called *effective*.

A *reduction* $\rho : C_* \twoheadrightarrow D_*$ between two chain complexes C_* and D_* is given by a triple $\rho = (f, g, h)$ where $f : C_* \to D_*$ and $g : D_* \to C_*$ are chain complex morphisms and h is a homotopy operator $h : C_* \to C_{*+1}$ satisfying some additional relations which ensure that the homology groups of C_* and D_* are canonically isomorphic (see [RS02] for details). Moreover, if the chain complexes C_* and D_* are endowed with I-filtrations F and F' respectively, we have proved that, under some good conditions of the reduction ρ, (some of the terms) of the spectral systems of (C_*, F) and (D_*, F') are isomorphic, so that we can compute the spectral system of the big chain complex C_* by using that of the small (finite type) chain complex D_*. More concretely, the following result expresses the conditions that are necessary to ensure that the spectral systems of the I-filtered chain complexes C_* and D_* are isomorphic and are used by our programs to compute the spectral system associated with chain complexes of infinite type.

Theorem 2.1. *Let $\rho = (f, g, h) : C_* \Rightarrow D_*$ be a reduction between the I-filtered chain complexes (C_*, F) and (D_*, F'), and suppose that f and g are compatible with the filtrations, that is, for all indices $i \in I$ one has $f(F_i) \subseteq F'_i$ and $g(F'_i) \subseteq F_i$. Then, given four indices $z \leq s \leq p \leq b$ in I, the map f induces an isomorphism between the spectral system terms:*

$$f^{z,s,p,b} : S[z, s, p, b] \to S'[z, s, p, b]$$

whenever the homotopy $h : C_* \to C_{*+1}$ satisfies the conditions $h(F_z) \subseteq F_s$ and $h(F_p) \subseteq F_b$.

3. Serre spectral system

One of the motivating examples of Matschke's work [Mat13] are *towers of fibrations*, that is, sequences of fibrations such that the total space of each is the base of the next one:

$$\begin{array}{ccc} G_0 & \longrightarrow & E_0 \\ & & \downarrow \\ \cdots & & \cdots \\ & & \downarrow \\ G_{m-1} & \longrightarrow & E_{m-1} \\ & & \downarrow \\ & & B \end{array} \tag{2}$$

In this situation, as the usual goal of computation is the homology $H(E_0)$ of the total space of the upper fibration, one typically applies several times the Serre spectral sequence [Ser51], assuming that the homology of $G_0, \ldots, G_{m-1}$ and B is known. Leaving aside extension problems, one can think to determine $H(E_{m-1})$ from $H(B)$ and $H(G_{m-1})$ via a first Serre spectral sequence, using then a second Serre spectral sequence to try to determine $H(E_{m-2})$ from $H(E_{m-1})$ and $H(G_{m-2})$ and so on. A suitably defined spectral system (in this case over the poset of *downsets* of $\mathbb{Z}^m$, denoted $D(\mathbb{Z}^m)$) represents a unified framework "containing" these spectral sequences and offering a larger number of connections to the limit $H(E_0)$. Moreover, the 2-page of the spectral system is defined by a formula which generalizes that of Serre's spectral sequence for a fibration.

Theorem 3.1. [Mat13] *Consider a tower of m fibrations. There exists an associated spectral system over $D(\mathbb{Z}^m)$ with 2-page*

$$H_{p_m}(B; H_{p_{m-1}}(G_{m-1}; \ldots H_{p_1}(G_1; H_{p_0}(G_0)))),$$

with $P = (p_1, \ldots, p_m) \in \mathbb{Z}^m$ and $p_0 = n - p_1 - \cdots - p_m$, which under suitable conditions converges to $H_n(E_0)$.

As in the classical case, this formula provides a description of the initial page of the generalized spectral sequence but the next terms $S[z, s, p, b]$ can only be determined in some simple cases. However, we can now try to use the effective homology of the space E_0 (which is built automatically by Kenzo when the spaces $G_0, \ldots, G_{m-1}$ and B are objects with effective homology) in order to determine the spectral system of the tower of fibrations by means of a spectral system associated with a chain complex of finite type.

Our study has begun with towers of fibrations without twist, that is, such that the space E_0 can be expressed as a cartesian product $E_0 \cong G_0 \times \cdots \times G_{m-1} \times B$. In this case

we have proved that generalized filtrations can be defined on E_0 and its associated chain complexes D_* and $\hat{C}_*$ obtained automatically by Kenzo such that the pair of reductions $C_*(E_0) \twoheadleftarrow \hat{C}_* \twoheadrightarrow D_*$ satisfy the hypotheses of Theorem 2.1 for terms $S[z, s, p, b]$ after level 2. In this way, we can compute the Serre spectral system of E_0 by using that of the effective chain complex D_*.

The case of towers of fibrations with twisting operators is more difficult because of the need of non-trivial generalizations of the involved filtrations. As a theme for further work, we are interested in trying to define suitable filtrations, in order to extend our method for computing the Serre spectral system to the twisted case.

4. Examples and computations

As an example of computation in the non-twisted case, we show the results of our programs for the Serre spectral system of the cartesian product $K(\mathbb{Z}_2, 2) \times K(\mathbb{Z}_2, 3) \times K(\mathbb{Z}, 4)$. Since it is a simplicial set of infinite type and therefore its spectral system cannot be directly determined, effective homology is used.

```
> (setf kz22 (k-z2 2) kz23 (k-z2 3) kz4 (k-z 4))
[K73 Abelian-Simplicial-Group]
> (setf K (crts-prdc (crts-prdc kz22 kz23) kz4))
[K90 Simplicial-Set]
> (setf Kf (change-chcm-to-gflcc K (dz2) crpr3-gflin 'crpr3-gflin))
[K97 Generalized-Filtered-Chain-Complex]
> (e2-gspsq-group K 4 0 4)
Generalized spectral sequence S[((0 2) (1 1) (2 0) (3 -1) (5 -2)),((0 3) (1 2)
  (2 1) (3 0) (5 -1)),((0 3) (1 2) (2 1) (4 0)),((0 4) (1 3) (2 2) (4 1) (5 0))]_{4}
Component Z/4Z
> (e2-gspsq-group K 0 5 5)
Generalized spectral sequence S[((1 3) (2 2) (3 1) (4 0)),((1 4) (2 3) (3 2)
  (4 1) (5 0)),((0 5) (1 4) (2 3) (3 2) (4 1) (5 0)),((0 6) (1 5) (2 4) (3 3) (4 2)
  (5 1) (6 0))]_{5}
Component Z/2Z
```

References

[DRSS99] X. Dousson, J. Rubio, F. Sergeraert, and Y. Siret. The Kenzo program. `http://www-fourier.ujf-grenoble.fr/~sergerar/Kenzo/`, 1999.

[GR18] A. Guidolin and A. Romero. Effective computation of generalized spectral sequences. 2018. Submitted.

[Mac63] S. MacLane. *Homology*. Springer, 1963.

[Mat13] B. Matschke. Successive spectral sequences, 2013. arXiv preprint arXiv:1308.3187.

[RS02] J. Rubio and F. Sergeraert. Constructive Algebraic Topology. *Bulletin des Sciences Mathématiques*, 126(5):389–412, 2002.

[Ser51] J. P. Serre. Homologie singulière des espaces fibrés. *Annals of Mathematics*, 54(3):425–505, 1951.

Politecnico di Torino. Cso Duca degli Abruzzi 24. 10129 Torino, Italy.
E-mail address: `andrea.guidolin@polito.it`

Universidad de La Rioja. c/Madre de Dios 53. 26006 Logroño, Spain.
E-mail address: `ana.romero@unirioja.es`

Monografías de la Real Academia de Ciencias. Zaragoza. **43:** 107–110, (2018).
ISSN: 1132-6360

A COMPUTATIONAL APPROACH TO KDV RATIONAL SOLITONS AND THEIR DIFFERENTIAL GALOIS GROUPS.

S. JIMÉNEZ, J. J. MORALES-RUIZ, R. SANCHEZ-CAUCE, AND M. A. ZURRO

Abstract. In this work we give explicit computations of the fundamental matrices associated to the Schrödinger operator $L = -\partial^2 + u$ for all values of the energy $E \in \mathbb{C}$, and for u the Adler-Moser solitons [1], that is u is a rational solution of the Korteweg-de Vries equation (KdV_1). Also we compute their differential Galois groups.

1. Introduction

In this paper we present a new framework to study and compute closed form solutions of the Schrödinger equation

$$(-\partial_{xx} + u)\Psi = E\Psi \tag{1}$$

for Adler-Moser rational potentials u in $1+1$ dimensions, [1]. These are a family of rational potentials $u_n = u_n(x,t)$ for Schrödinger operator $L = -\partial_{xx} + u$ of the form $u_n = -2(\log\theta_n)_{xx}$, where θ_n are rational functions in the variables (x,t) defined by some differential recursion (see (5)).

The stationary problem associated to (1) is the equation $(-\partial_{xx} + \frac{2}{x^2})\Psi = E\Psi$ (see [2]). Its (affine) spectral curve, $f(E,\mu) = \mu^2 + E^3$, is in the basis of the understanding of the closed formulas given in our result 2.1. This simple curve allows the study of the closed formulas previously mentioned depending on the type of point of the curve on which we are working on. Thus, when the point is singular, that is, when the energy E is zero, it is easy to recover the Adler-Moser formulas for the fundamental matrix of solutions of (1). The rest of affine points of this curve are non singular and the fundamental matrix has a similar behavior on all of them (case $E \neq 0$). As a consequence of our work we can compute the Picard-Vessiot extension associated with the problem (1) for any value of the energy E. In the talk we will also present a general framework to compute the differential Galois group of the Schrödinger operator with rational potential in the KdV hierarchy.

We consider this work a first part of a project devoted to develop the Differential Galois Theory of Schrödinger equations for general solitonic potentials in $1+1$ dimensions, [3].

2. KdV rational Schrödinger operator and its differential Galois group

Let K be a differential field with compatible derivations $\partial_x, \partial_{t_1}, \partial_{t_2}, \ldots, \partial_{t_m}$ with respect to the variables x and $t = (t_1, \ldots, t_m)$, and field of constants C algebraically closed and of characteristic zero. Let E be a parameter and $u = u(x,t)$ be a fixed element of the differential field K.

Second author partially supported by the research group Modelos Matemáticos no Lineales, UPM.
Fourth author partially supported by Grupo UCM 910444.

Consider the Schrödinger operator $L = -\partial_{xx} + u$ and the Schrödinger equation

$$(L - E)\phi = (-\partial_{xx} + u - E)\phi = 0. \tag{2}$$

It is well known that the time dependent KdV hierarchy can be constructed as zero curvature condition of the family of integrable systems (see [2] chapter 1, section 2):

$$\Phi_x = U\Phi = \begin{pmatrix} 0 & 1 \\ u - E & 0 \end{pmatrix} \Phi\,, \qquad \Phi_{t_r} = V_r\Phi = \begin{pmatrix} -\frac{F_{r,x}(u)}{2} & F_r(u) \\ (u-E)F_r - \frac{F_{r,xx}}{2} & \frac{F_{r,x}(u)}{2} \end{pmatrix} \Phi\,, \tag{3}$$

where F_r is a differential polynomial of the potential u defined by $F_r = \sum_{j=0}^{r} f_{r-j}E^j$ where the f_i are given by the recursive relations $f_0 = 1$ and $f_{j,x} = -\frac{1}{4}f_{j-1,xxx} + uf_{j-1,x} + \frac{1}{2}u_x f_{j-1}$.

Now, fix a level r in the hierarchy and consider the corresponding system (3). Its zero curvature condition, $U_{t_r} - V_{r,x} + [U, V_r] = 0$, yields to the KdV_r equation of the KdV hierarchy:

$$\mathrm{KdV}_r: \quad u_{t_r} = 2f_{r+1,x} = -\tfrac{1}{2}F_{r,xxx} - 2(E-u)F_{r,x} + u_x F_r. \tag{4}$$

In this paper we will focus on the first KdV equation, that is $r = m = 1$, and hence we will put $t = t_1$ from now on. Also, the differential field K will be $C(x,t)$. Adler and Moser constructed in [1] a family of KdV rational potentials $u_n = u_n(x,t)$ for the Schrödinger operator $-\partial_{xx} + u$ where $u_n = -2(\log\theta_n)_{xx}$, for θ_n functions in the variables x, t defined by the differential recursion:

$$\theta_0 = 1, \qquad \theta_1 = x, \qquad \theta_{n+1,x}\theta_{n-1} - \theta_{n+1}\theta_{n-1,x} = (2n+1)\theta_n^2. \tag{5}$$

Its solutions are polynomials in x with coefficients in the field $C(t)$, for instance,

$$\theta_2 = x^3 + \tau_2 \qquad \text{and} \qquad \theta_3 = x^6 + 5\tau_2 x^3 + \tau_3 x - 5\tau_2^2,$$

for τ_2 and τ_3 integration constants of x.

For $E = 0$, Adler and Moser in [1] have computed the fundamental matrices of system (3) for the rational soliton $u_n = -2(\log\theta_n)_{xx}$, say

$$\mathcal{B}_{n,0} = \begin{pmatrix} \phi_{1,n} & \phi_{2,n} \\ \phi_{1,n,x} & \phi_{2,n,x} \end{pmatrix},$$

where $\phi_{1,n} = \frac{\theta_{n-1}}{\theta_n}$, $\phi_{2,n} = \frac{\theta_{n+1}}{\theta_n}$ are in K. So, the Picard-Vessiot field of (3) is again K, i.e., there is no differential extension. Thus, the differential Galois group is $G_{n,0} = \{\mathrm{id}\}$.

2.1. **Fundamental matrices for $E \neq 0$.** In this section, we compute explicitly fundamental matrices of system (3) when $u = u_n = -2(\log\theta_n)_{xx}$ and $E \neq 0$. The system is:

$$\begin{cases} \Phi_x &= U\Phi = \begin{pmatrix} 0 & 1 \\ u_n - E & 0 \end{pmatrix}\Phi, \\ \Phi_t &= V\Phi = \begin{pmatrix} -\frac{u_{n,x}}{4} & E + \frac{u_n}{2} \\ -E^2 + \frac{Eu_n}{2} + \frac{u_n^2}{2} - \frac{u_{n,xx}}{4} & \frac{u_{n,x}}{4} \end{pmatrix}\Phi. \end{cases} \tag{6}$$

The zero curvature condition of this system is still the KdV_1 equation:

$$u_{n,t} = \frac{3}{2}u_n u_{n,x} - \frac{1}{4}u_{n,xxx}. \tag{7}$$

When $E \neq 0$, we take $\lambda \in C$ a parameter over K such that $E + \lambda^2 = 0$. We have the following result:

Theorem 2.1. *Let n be a non negative integer. For $E = -\lambda^2 \neq 0$ and $u = u_n$ a fundamental matrix for system (6) is:*

$$\mathcal{B}_{n,\lambda} = \begin{pmatrix} \phi_n^+ & \phi_n^- \\ \phi_{n,x}^+ & \phi_{n,x}^- \end{pmatrix}, \tag{8}$$

where $\phi_n^+(x,t,\lambda) = \dfrac{e^{\lambda x - \lambda^3 t} Q_n^+(x,t,\lambda)}{\theta_n}$ and $\phi_n^-(x,t,\lambda) = \dfrac{e^{-\lambda x + \lambda^3 t} Q_n^-(x,t,\lambda)}{\theta_n}$, where $Q_n^\pm$ are rational functions in x, t, λ such that they are solution of the following differential systems:

$$Q_{n,xx}^\pm = Q_{n,x}^\pm \left(\mp 2\lambda + 2\frac{\theta_{n,x}}{\theta_n} \right) + Q_n^\pm \left(\pm 2\lambda \frac{\theta_{n,x}}{\theta_n} - \frac{\theta_{n,xx}}{\theta_n} \right), \tag{9}$$

$$\begin{aligned} Q_{n,t}^\pm = {} & Q_{n,x}^\pm \left(-\lambda^2 - \frac{\theta_{n,xx}}{\theta_n} + \frac{\theta_{n,x}^2}{\theta_n^2} \right) + \\ & + Q_n^\pm \left(\lambda^2 \frac{\theta_{n,x}}{\theta_n} \pm \lambda \frac{\theta_{n,x}^2}{\theta_n^2} \mp \lambda \frac{\theta_{n,xx}}{\theta_n} + \frac{\theta_{n,xxx}}{2\theta_n} - \frac{\theta_{n,x}\theta_{n,xx}}{2\theta_n^2} + \frac{\theta_{n,t}}{\theta_n} \right). \end{aligned} \tag{10}$$

Remark 2.2. *It is always possible to obtain a closed form solution of differential system (9) and (10) computationally. Therefore, we can compute fundamental matrices $\mathcal{B}_{n,\lambda}$ for each n.*

Remark 2.3. *From Theorem 2.1 we can compute the determinant:* $\det(\mathcal{B}_{n,\lambda}) = -2\lambda^{2n+1}$.

Proof. We proceed to sketch the proof. It will follows by induction on n. For $n = 0$ we have $u_0 = 0$. Hence, $\phi_0^+ = e^{\lambda x - \lambda^3 t}$ and $\phi_0^- = e^{-\lambda x + \lambda^3 t}$, and we get the desire formulas for $\mathcal{B}_{\lambda,0}$.

Now, we will compute $\mathcal{B}_{n+1,\lambda}$. We apply a Darboux transformation with $\phi_{2,n} = \frac{\theta_{n+1}}{\theta_n}$ to solutions $\phi_n^+(x,t,\lambda)$ and $\phi_n^-(x,t,\lambda)$ and we obtain

$$\begin{aligned} DT(\phi_{2,n})\phi_n^+ &= \phi_{n,x}^+ - \tfrac{\phi_{2,n,x}}{\phi_{2,n}}\phi_n^+ = \tfrac{e^{\lambda x - \lambda^3 t}}{\theta_{n+1}} \cdot \tfrac{\lambda Q_n^+ \theta_{n+1} + Q_{n,x}^+ \theta_{n+1} - Q_n^+ \theta_{n+1,x}}{\theta_n}, \\ DT(\phi_{2,n})\phi_n^- &= \phi_{n,x}^- - \tfrac{\phi_{2,n,x}}{\phi_{2,n}}\phi_n^- = \tfrac{e^{-\lambda x + \lambda^3 t}}{\theta_{n+1}} \cdot \tfrac{-\lambda Q_n^- \theta_{n+1} + Q_{n,x}^- \theta_{n+1} - Q_n^- \theta_{n+1,x}}{\theta_n}. \end{aligned}$$

They are solutions of Schrödinger equation for $E \neq 0$ and potential $DT(\phi_{2,n})u_n = u_n - 2(\log \phi_{2,n})_{xx} = u_{n+1}$. Now, we define the expressions

$$Q_{n+1}^+ := \tfrac{\lambda Q_n^+ \theta_{n+1} + Q_{n,x}^+ \theta_{n+1} - Q_n^+ \theta_{n+1,x}}{\theta_n}, \quad Q_{n+1}^- := \tfrac{-\lambda Q_n^- \theta_{n+1} + Q_{n,x}^- \theta_{n+1} - Q_n^- \theta_{n+1,x}}{\theta_n}.$$

A long computation shows that these functions verify the differential equations (9) and (10) for $n+1$. This ends the proof. □

2.2. **Differential Galois groups for $E \neq 0$.** The Picard-Vessiot extension of the differential system (6) is given by the fundamental matrix $\mathcal{B}_{n,\lambda}$ as in 2.1 whose entries are in $K(e^{\lambda x - \lambda^3 t})$. To compute its differential Galois group $G_{n,\lambda}$ we just have to compute the action of each $\sigma \in G_{n,\lambda}$ on $e^{\lambda x - \lambda^3 t}$. Since $\partial_x \left(\frac{\sigma(e^{\lambda x - \lambda^3 t})}{e^{\lambda x - \lambda^3 t}} \right) = 0$, and $\partial_t \left(\frac{\sigma(e^{\lambda x - \lambda^3 t})}{e^{\lambda x - \lambda^3 t}} \right) = 0$,

we have $\sigma(e^{\lambda x-\lambda^3 t}) = c \cdot e^{\lambda x-\lambda^3 t}$ for some constant $c \in C$. Therefore, the differential Galois group is isomorphic to the multiplicative group: $G_{n,\lambda} \simeq G_m = \left\{ \begin{pmatrix} c & 0 \\ 0 & c^{-1} \end{pmatrix} : c \in C^* \right\}$.

3. Some explicit examples

Next we compute fundamental solutions for Schrödinger operators with potentials u_n and energy level $E = -\lambda^2 \neq 0$ for $n = 0, 1, 2$ and 3. All computations were made with SAGE.

u_n	ϕ_n^+	ϕ_n^-
0	$e^{\lambda x-\lambda^3 t}$	$e^{-\lambda x+\lambda^3 t}$
$\frac{2}{x^2}$	$\frac{e^{\lambda x-\lambda^3 t}(\lambda x-1)}{x}$	$\frac{e^{-\lambda x+\lambda^3 t}(\lambda x+1)}{x}$
$\frac{6x(x^3-6t)}{(x^3+3t)^2}$	$\frac{e^{\lambda x-\lambda^3 t}(\lambda^2 x^3-3\lambda x^2+3x+3\lambda^2 t)}{x^3+3t}$	$\frac{e^{-\lambda x+\lambda^3 t}(\lambda^2 x^3+3\lambda x^2+3x+3\lambda^2 t)}{x^3+3t}$

Next, we consider the potential $u_3 = \frac{6x(2x^9+675x^3t^2+1350t^3)}{(x^6+15x^3t-45t^2)^2}$. We can construct the solutions:

$$\phi_3^+ = \frac{e^{\lambda x-\lambda^3 t} Q_3^+(\lambda, x, t)}{x^6+15x^3t-45t^2}\ , \qquad \phi_3^- = \frac{e^{-\lambda x+\lambda^3 t} Q_3^-(\lambda, x, t)}{x^6+15x^3t-45t^2}$$

where

$$\begin{aligned} Q_3^+(\lambda, x, t) =& \lambda^3 x^6 - 6\lambda^2 x^5 + 15\lambda x^4 - 15x^3 + 15\lambda^3 x^3 t - 45\lambda^2 x^2 t + 45\lambda x t - 45\lambda^3 t^2 - 45t, \\ Q_3^-(\lambda, x, t) =& \lambda^3 x^6 + 6\lambda^2 x^5 + 15\lambda x^4 + 15x^3 + 15\lambda^3 x^3 t + 45\lambda^2 x^2 t + 45\lambda x t - 45\lambda^3 t^2 + 45t. \end{aligned}$$

References

[1] M. Adler, J. Moser, On a Class of Polynomials Connected with the Korteweg-de Vries Equation, Commun. math. Phys. 61, 1-30 (1978).

[2] F. Gesztesy, H. Holden, Soliton Equations and Their Algebro-Geometric Solutions, Volume 1: (1+1)-Dimensional Continuous Models, Cambridge Stud. Adv. Math., Vol. 79, Cambridge Univ. Press, (2003).

[3] S. Jiménez, J. J. Morales-Ruiz,R. Sánchez-Cauce, M. A. Zurro, Differential Galois theory and Darboux transformations for integrable systems. Journal of Geometry and Physics 115 (2017), 75-88.

Junta de Castilla y León
E-mail address: sonia.jimver@educa.jcyl.es

Universidad Politécnica de Madrid
E-mail address: juan.morales-ruiz@upm.es

Universidad Autónoma de Madrid
E-mail address: raquel.sanchezcauce@predoc.uam.es

Universidad Autónoma de Madrid
E-mail address: mangeles.zurro@uam.es

Monografías de la Real Academia de Ciencias. Zaragoza. **43:** 111–114, (2018).
ISSN: 1132-6360

ENUNCIADOS NI CIERTOS NI FALSOS EN RAZONAMIENTO AUTOMÁTICO EN GEOMETRÍA

ZOLTÁN KOVÁCS, TOMÁS RECIO Y M. PILAR VÉLEZ

Abstract. We investigate and generalize to an extended framework the notion of *true on components* labeled by Zhou, Wang and Sun in their paper "Automated Reducible Geometric Theorem Proving and Discovery by Gröbner Basis Method", J. Automat. Reasoning 59 (3), 331-344, 2017. A new, simple criterion is presented for a statement to be simultaneously not generally true and not generally false (i.e. true on components), and its performance is exemplified through the implementation of this test in the dynamic geometry program GeoGebra. This extended abstract is based on a recent work by the authors [5].

Introducción

El enfoque de razonamiento automático basado en geometría algebraica consiste en traducir los enunciados de geometría elemental, $\{H \Rightarrow T\}$, a expresiones algebraicas. De este modo los objetos geométricos que verifican las hipótesis son soluciones de un sistema de polinomios $V(H) = \{h_1 = 0, \ldots, h_r = 0\}$ (variedad de hipotésis), y se representan algebraicamente por estos polinomios como un ideal (de hipótesis), $H = \langle h_1 \ldots, h_r \rangle$, en un anillo de polinomios. Igualmente la tesis es solución de una ecuación $V(T) = \{f = 0\}$.

Cuando $V(H) \subseteq V(T)$ podemos decir que el teorema es *siempre cierto*. Sin embargo, esto sucede raras veces, incluso para teoremas bien conocidos, dado que la traducción algebraica del enunciado geométrico no suele excluir los casos degenerados, ver por ejemplo [3].

Por ello se hace un planteamiento ligeramente diferente, detectar primero una colección de variables tal que ninguna relación polinómica entre estas variables se anule sobre todo $V(H)$ (i.e. variables independientes módulo H). Entonces, las componentes irreducibles de $V(H)$ sobre las que estas variables permanecen independientes se denominan *no degeneradas*.

Así, un enunciado es *generalmente cierto* si la tesis se verifica al menos sobre todas las componentes no degeneradas. Y si la tesis no se anula idénticamente sobre ninguna componente no degenerada el enunciado se considera *generalmente falso*. Observar que esto incluye el caso *siempre falso* en que la tesis no se verifica sobre ningún punto de la variedad de hipótesis.

En este contexto se presenta un caso particular que se ha revelado de gran interés, aquellos enunciados que resultan no ser ciertos ni falsos.

Analicemos un ejemplo muy simple. Sean los puntos del plano $A(0,0), B(2,0)$ y las circunferencias c centrada en A y d centrada en B, ambas de radio $r = \sqrt{3}$, i.e. $c : x^2 + y^2 - 3 = 0$

Date: Febrero de 2018.

Partially supported by the Spanish Research Project MTM2017-88796-P Computación simbólica: nuevos retos en álgebra y geometría y sus aplicaciones.

and $d : (x-2)^2 + y^2 - 3 = 0$. Tomemos $E(u,v)$ y $F(m,n)$ los puntos de intersección de c y d. El ideal de hipótesis es: $\langle u^2+v^2-3, (u-2)^2+v^2-3, m^2+n^2-3, (m-2)^2+n^2-3\rangle$.

La tesis de este enunciado es que las rectas AE y BF son paralelas, es decir, viene dada por el polinomio: $u \cdot n - v \cdot (m-2)$.

El ideal de hipótesis es claramente de dimensión cero y tiene dos componentes primarias sobre los racionales,

$$\begin{aligned}&\langle v-n, (m-2)^2+n^2-3, (u-2)^2+v^2-3, m^2+n^2-3, u^2+v^2-3\rangle = \\ &\qquad = \langle v-n, u-1, m-1, n^2-2\rangle \\ &\langle v+n, (m-2)^2+n^2-3, (u-2)^2+v^2-3, m^2+n^2-3, u^2+v^2-3\rangle = \\ &\qquad = \langle v+n, u-1, m-1, n^2-2\rangle .\end{aligned}$$

Es fácil verificar que la tesis es falsa sobre la primera componente y cierta sobre la segunda. Se trata por tanto de un enunciado de geometría elemental que con este enfoque, podríamos decir, no es ni cierto ni falso.

Por definición un enunciado no puede ser a la vez generalmente cierto y generalmente falso. Sin embargo, como muestra el ejemplo anterior, existen enunciados que son a la vez no generalmente ciertos y no generalmente falsos (otros ejemplos en [6, 1]).

Por otra parte, obsérvese que los conceptos introducidos arriba aluden a componentes irreducibles de una variedad algebraica y a un conjunto de variables independientes, por tanto dependen por una parte del cuerpo base sobre el que trabajemos (el ideal H del ejemplo anterior tiene cuatro componentes sobre $\mathbb{Q}(\sqrt{2})$) y, por otra, del conjunto de variables independientes elegido.

Los resultados que aquí presentamos a continuación forman parte de un reciente trabajo de los autores [5] sobre las cuestiones mencionadas arriba.

1. Enunciados generalmente ciertos en componentes

Sean K y L cuerpos, con L extensión algebraicamente cerrada de K (por ejemplo $L = \mathbb{C}$ y $K = \mathbb{Q}$) y considérese un enunciado $\{H \Rightarrow T\}$. Sean $H = \langle h_1 \ldots, h_r\rangle$ y $T = \langle f\rangle$ los ideales de hipótesis y de tesis en un anillo de polinomios $K[X]$, donde las variables $X = \{x_1, \ldots, x_n\}$ se refieren a las coordenadas utilizadas en la descripción algebraica de las hipótesis. Y sean $V(H)$ y $V(T)$ las correspondientes variedades de hipótesis y de tesis en el espacio afín L^n definidas sobre K.

En lo que sigue fijemos un enunciado $\{H \Rightarrow T\}$ formulado sobre K y un subconjunto $Y = \{x_1, \ldots, x_d\}$ de X de variables independientes para H (i.e. $H \cap K[Y] = \langle 0\rangle$).

Definición 1.1. El enunciado es *generalmente cierto* si la tesis f se anula idénticamente en todas las K-componentes de $V(H)$ no degeneradas con respecto Y.
El enunciado es *generalmente falso* si la tesis f no se anula idénticamente sobre ninguna las K-componentes de $V(H)$ no degeneradas con respecto Y.

La terminología "cierto en componentes" ha sido introducido recientemente en [7] para enunciados que no son generalmente ciertos ni falsos, pero en un contexto ligeramente diferente al nuestro, suponiendo $K = L$ algebraicamente cerrado.

Definición 1.2. El enunciado es *cierto en componentes* (o *cierto en partes no degeneradas*) si la tesis f se anula identicamente en alguna, pero no todas las K-componentes de $V(H)$ en L^n no degeneradas para Y; es decir, si no es ni generalmente cierto, ni generalmente falso.

Tómese ahora $Y = \{x_1, \ldots, x_d\}$ $(0 \leq d \leq n)$ *un conjunto de variables independientes de cardinal máximo* para el ideal de hipótesis H; esto es $H \cap K[Y] = \langle 0 \rangle$ y para cualquier conjunto $Z \subset X$ con $r > d$ elementos, $H \cap K[Z] \neq \langle 0 \rangle$. Luego, la dimensión de Krull de $V(H)$ es d.

En [6] se da una condición necesaria y suficiente para enunciados generalmente ciertos y otra para generalmente falsos, basadas ambas en eliminación en ideales de polinomios. En [5] se retoma esta idea y se demuestra el siguiente teorema.

Teorema 1.3. *Sea $\{H \Rightarrow T\}$ un enunciado y establezcamos un conjunto de variables independientes de cardinal máximo $Y = \{x_1, \ldots, x_d\}$ para el ideal H (i.e. $d = \dim(H)$). Entonces, el enunciado es cierto en componentes si y sólo si*

$$(i)\ \langle h_1, \ldots, h_r, f \cdot t - 1 \rangle\, K[X,t] \cap K[Y] = \langle 0 \rangle\,, \text{ y}$$
$$(ii)\ \langle h_1, \ldots, h_r, f \rangle\, K[X] \cap K[Y] = \langle 0 \rangle\,.$$

El teorema anterior proporciona un criterio directo para detectar si un enunciado es cierto en componentes comprobando si el resultado de dos eliminaciones es cero o no. La primera detecta que el enunciado es no generalmente cierto y la segunda que es no generalmente falso, además ambas condiciones son necesarias y suficientes (ver [6]).

Por otra parte, este teorema nos permite también entender un hecho aparentemente contradictorio que se ha señalado anteriormente: la descomposición primaria de un ideal depende del cuerpo base. Sin embargo, teniendo en cuenta que el cálculo de bases de Gröbner (fundamento de los algoritmos de eliminación) se realiza sobre el cuerpo base, podemos deducir el siguiente:

Corolario 1.4. *Sea K' un cuerpo intermedio, $K \subseteq K' \subseteq L$, donde L es algebraicamente cerrado. En las hipótesis del teorema, un enunciado es* cierto en K-componentes *si y sólo si es* cierto en K'-componentes*; es decir, el concepto* cierto en componentes *no depende de las extensiones del cuerpo base.*

Nota 1.5. Cuando trabajamos con enunciados de geometría parece lógico tomar como variables independientes las coordenadas de los puntos libres de la configuración geométrica que estamos tratando. En la mayoría de los casos este conjunto de variables "intuitivamente" maximal es de cardinal máximo, pero hay ejemplos en los que no es así. Por ejemplo en [3, Ejemplo 7], se construye un triángulo de vértices $(-1,0), (1,0), (u[1], u[2])$ para razonar sobre la fórmula de Euler que relaciona los radios de las circunferencias inscrita y circunscrita. Aquí la dimensión esperada es 2, pero la dimensión del ideal de hipótesis es 3. Sin embargo, si se incluye como nueva hipótesis que $(u[1], u[2])$ no esté en el eje x se obtiene la dimensión 2. Se trata de un problema relacionado con la dificultad de controlar todas las degeneraciones cuando se trabaja algebraicamente que ya fue considerado en [2].

Obviamente el hecho de que las coordenadas de los puntos libres de la configuración geométrica sean un conjunto de variables independientes de cardinal máximo para H da sentido a los conceptos de generalmente cierto, generalmente falso y cierto en componentes. Por ello, cuando esto no sucede, proponemos revisar la construcción evitando degeneraciones.

2. Implementación en GeoGebra

El programa de geometría dinámica GeoGebra incluye, entre sus utilidades de razonamiento automático, el concepto "cierto en componentes" desde la versión 5.0.415.0 (diciembre

2017), ver [4]. El criterio del Teorema 1.3 nos ha permitido completar los casos de decisión sobre la veracidad de enunciados de geometría elemental.

A continuación se presentan a grandes rasgos los pasos de este algoritmo para decidir la veracidad de un enunciado $\{H \Rightarrow T\}$:

1) Primero elegir en la construcción un conjunto Y de variables geométricamente independientes entre las coordenadas de los puntos libres de la configuración y comprobar que realmente son independientes, $H \cap K[Y] = \langle 0 \rangle$.

2) Comprobar si la dimensión de Hilbert de H coincide con el cardinal de Y. Si no es así se sugiere al usuario *revisar degeneraciones en la construcción* (FIN). En otro caso continuar.

3) Calcular $\langle h_1, \ldots, h_r, f \cdot t - 1 \rangle\, K[X,t] \cap K[Y]$. Si es $\neq \langle 0 \rangle$ el enunciado es *generalmente cierto* (FIN). En otro caso continuar.

4) Calcular $\langle h_1, \ldots, h_r, f \rangle\, K[X] \cap K[Y]$. Si es $\neq \langle 0 \rangle$ el enunciado es *generalmente falso* (FIN). En otro caso el enunciado es *cierto en componentes*(En este caso la respuesta de GeoGebra es *verdadero en parte, falso en parte*).

Sobre lo expuesto anteriormente, pueden consultarse varios ejemplos ilustrativos en `https://www.geogebra.org/m/zpDq7taB`.

Referencias

[1] Botana, F., Recio, T.: On the unavoidable uncertainty of truth in dynamic geometry proving, Mathematics in Computer Science, 10(1), 5-25 (2016).

[2] Chou, S.C.: Mechanical geometry theorem proving, Mathematics and its Applications, vol. 41. D. Reidel Publishing Co., Dordrecht (1988), with a foreword by Larry Wos.

[3] Dalzotto, G., Recio, T.: On protocols for the automated discovery of theorems in elementary geometry, Journal of Automated Reasoning, 43, 203-236 (2009).

[4] Kovács, Z., Recio, T., Vélez, M.P.: GeoGebra automated reasoning tools: a tutorial. Available at https://github.com/kovzol/gg-art-doc/blob/master/pdf/english.pdf

[5] Kovács, Z., Recio, T., Vélez, M.P.: Detecting true on components. Preprint. arXiv: 1802.05875 [cs.AI] (2018).

[6] Recio, T., Vélez, M.P.: Automatic discovery of theorems in elementary geometry, Journal of Automated Reasoning, 23, 63-82 (1999).

[7] Zhou, J., Wang, D., Sun, Y.: Automated reducible geometric theorem proving and discovery by Gröbner basis method, Journal of Automated Reasoning, 59(3), 331-344 (2017).

Private Pädagogische Hochschule der Diözese Linz, Linz (Austria)
E-mail address: `zoltan@geogebra.org`

Universidad de Cantabria, Santander (España)
E-mail address: `tomas.recio@unican.es`

Universidad Antonio de Nebrija, Madrid (España)
E-mail address: `pvelez@nebrija.es`

Monografías de la Real Academia de Ciencias. Zaragoza. **43:** 115–118, (2018).
ISSN: 1132-6360

CONSTRUCTING QUATERNION AND SYMBOL DIVISION ALGEBRAS WITH GIVEN INVARIANTS

PÉTER KUTAS

Abstract. We propose randomized polynomial time algorithms for constructing quaternion algebras and symbol algebras with prescribed invariants. The key ingredient of these algorithms is an effective function field version of Dirichlet's theorem on arithmetic progressions. We apply our algorithms to compute primitive idempotents in central simple $\mathbb{F}_q(t)$-algebras given by structure constants.

Introduction

Dirichlet's theorem states that there are infinitely many prime numbers in an arithmetic progression, provided the first element and the difference are coprime. The analogous statement is true for monic irreducible polynomials in $\mathbb{F}_q[t]$. However, in the function field case a much stronger theorem holds. One can give a good estimation (depending on the degree of the difference of the arithmetic progression) on the number of irreducible polynomials in a residue class ([9, Theorem 5.1.]):

Theorem 0.1. *Let $a, m \in \mathbb{F}_q[t]$ be such that $deg(m) > 0$ and the $gcd(a, m) = 1$. Let N be a positive integer and let*

$$S_N(a, m) = \#\{f \in \mathbb{F}_q[t] \text{ monic irreducible } \mid f \equiv a \ (mod\ m),\ deg(f) = N\}.$$

Let $M = deg(m)$ and let $\Phi(m)$ denote the number of polynomials in $\mathbb{F}_q[t]$ relative prime to m whose degree is smaller than M. Then we have the following inequality:

$$|S_N(a, m) - \frac{q^N}{\Phi(m)N}| \leq \frac{1}{N}(M + 1)q^{\frac{N}{2}}.$$

Theorem 0.1 implies that choosing an irreducible polynomial from a residue class modulo f (a monic irreducible polynomial) can be done in the following fashion. One chooses a degree m which is sufficiently large (four times the degree of f suffices) and then a random polynomial of the given residue class of degree m will be irreducible with high probability. In [6] the authors use this fact to design an algorithm for finding nontrivial zeros of quadratic forms over $\mathbb{F}_q(t)$ in four or more variables.

Here we use this method to construct quaternion and symbol division algebras with prescribed invariants. In [1] the same task is addressed for general cyclic algebras (symbol algebras are cyclic algebras where it is assumed that the ground field contains the nth roots of unity). They propose a randomized polynomial time algorithm provided the Hasse invariant at infinity is zero. Our goal is to propose a randomized polynomial time algorithm where the Hasse invariant at infinity is not necessarily zero (however, we assume that $\mathbb{F}_q$ contains the nth roots of unity).

We apply our algorithms to solve the following problem. Let A be a cyclic algebra over $\mathbb{F}_q(t)$. The task is to find a primitive idempotent in A. We note that if $A \cong M_n(\mathbb{F}_q(t))$, then there exists a randomized polynomial time algorithm which finds a primitive idempotent

in A [5]. This problem was motivated by coding theory. In [2] the authors propose a new perspective on cyclicity concerning convolutional codes. They construct skew-cyclic codes of designated Hamming distance and propose an efficient decoding algorithm [3]. Finding primitive idempotents in cyclic algebras can be applied to construct constacyclic convolutional codes of designated Hamming distance.

1. Main results

Definition 1.1. Let K be a field such that $char(K) \neq 2$. Then a central simple algebra of dimension 4 over K is called a quaternion algebra.

A quaternion algebra H always admits a K-basis $1, u, v, uv$ such that

$$u^2 = a,\ v^2 = b,\ uv + vu = 0$$

where $a, b \in K^*$. A quaternion algebra is either a division algebra or it is isomorphic to $M_2(K)$.

Definition 1.2. Let H be a quaternion algebra over K. Let v be a place of K. We say that H is split at the place v if $H \otimes K_v$ is isomorphic to $M_2(K_v)$ (K_v denotes the completion of K at v).

If K is a global field (i.e., a finite extension of $\mathbb{Q}$ or $\mathbb{F}_q(t)$), then the isomorphism class of the quaternion algebra is determined by the list of places at which it does not split. Note that, due to Hilbert reciprocity, the number of places at which a quaternion algebra does not split is always even (and is, in particular, finite).

Our first result is a randomized algorithm which constructs a quaternion algebra over $\mathbb{F}_q(t)$, where q is odd, with prescribed splitting at given places:

Theorem 1.3. *Assume that S is a finite (non-empty) set of places of $\mathbb{F}_q(t)$. Then there exists a randomized polynomial time algorithm (polynomial in d and $\log\ q$) which constructs a quaternion division algebra H such that $H \otimes \mathbb{F}_q(t)_v$ is split if and only if $v \notin S$ if such a quaternion algebra exists.*

Remark 1.4. We sketch the key ingredients of the algorithm. We look for a quaternion algebra with parameters (a, b), where

$$a = f_1 \cdots f_k s,\ b = f_1 \cdots f_k \lambda,$$

where the f_i are the finite places at which H does not split, λ is an element from $\mathbb{F}_q$ and s is a suitable monic irreducible polynomial in $\mathbb{F}_q[t]$. Thus the algorithm boils down to finding a suitable s and λ. If H is in this form, then it splits at all finite places different from the f_i and s. The condition of splitting or not splitting at infinity can be achieved by choosing λ and the degree parity of s in a suitable way. Not splitting at the places f_i invokes congruence conditions on s. This means that one needs an s whose degree parity and residue modulo $f_1 \cdots f_k$ is fixed. This can be done by choosing a large enough degree and picking a polynomial from the residue class at random. Theorem 0.1 implies that this procedure is effective.

Symbol algebras are generalizations of quaternion algebras for arbitrary degree n with the extra assumption that the ground field K contains the nth roots of unity (note that this assumption is also needed for quaternion algebras as we excluded ground fields of characteristic 2).

Definition 1.5. Let K be a field which contains the nth roots of unity. Let ϵ be a primitive nth root of unity in K. Then a symbol algebra is an algebra generated by u, v which satisfies the following conditions:

$$u^n = a,\ v^n = b,\ uv = \epsilon vu.$$

Remark 1.6. Symbol algebras are a special case of cyclic algebras. Indeed, $L = K(b^{\frac{1}{n}})$ is a cyclic extension which splits the algebra. Moreover, conjugation by u induces the automorphism of L which sends $b^{\frac{1}{n}}$ to $\epsilon b^{\frac{1}{n}}$.

We recall some facts about central simple algebras over local and global fields [7],[8].

Theorem 1.7. *Let K be a local field (i.e., a complete field with respect to a discrete valuation and finite residue field). Then a central simple algebra over K is Brauer equivalent to a cyclic algebra $(W|K, a, \sigma)$ where W is an unramified cyclic extension of K and σ is the lift of the Frobenius map.*

Definition 1.8. Let K be a local field with valuation v. Then the Hasse invariant of the cyclic algebra $A = (W|K, a, \sigma)$ is $\frac{v(a)}{n}$, where n is the degree of A.

Central simple algebras over local fields are completely characterized by their Hasse invariants. Central simple algebras over global fields are determined by their local Hasse invariants. The Hasse invariant is zero at all but finitely many places and the sum of the nonzero Hasse invariants is an integers. This can be summarized in the following exact sequence:

Theorem 1.9. *Let K be a global field. Let $Br(K)$ denote the Brauer group of K. Then the following sequence is exact:*

$$0 \to Br(K) \to \bigoplus_v Br(K_v) \to \mathbb{Q}/\mathbb{Z} \to 0.$$

As a generalization of Theorem 1.3 we propose an algorithm for constructing symbol division algebras with prescribed Hasse invariants:

Theorem 1.10. *Let $\mathbb{F}_q$ be a finite field which contains the nth roots of unity. Assume that we are given a set of monic irreducible polynomials $f_1, \ldots, f_k$ (in $\mathbb{F}_q[t]$) and a sequence of rational numbers (in reduced form) $\frac{r_1}{s_1}, \ldots, \frac{r_k}{s_k}, \frac{r_\infty}{s_\infty}$. Suppose that the sum of these rational numbers is an integer. Assume that the least common multiple of the s_i is n . Then there exists a randomized polynomial time algorithm which constructs a division $\mathbb{F}_q(t)$-algebra of degree n, whose local Hasse invariant at f_i is equal to $\frac{r_i}{s_i}$, the local Hasse invariant at infinity is equal to $\frac{r_\infty}{s_\infty}$ and the local Hasse invariant at every other place is 0.*

Remark 1.11. We look for a and b in the form

$$a = s,\ b = f_1 \cdots f_k g\lambda,$$

where s and g are suitable irreducible polynomials and $\lambda \in \mathbb{F}_q$. The Hasse invariant can be computed easily as $\mathbb{F}_q(t)_v(s^{\frac{1}{n}})$ is an unramified splitting field of the symbol algebra. Thus again by choosing λ in a suitable fashion and choosing s from a suitable residue class and of a suitable degree we have that the algebra has the prescribed invariants. The extra polynomial g is only needed if the degree of $f_1 \cdots f_k$ is not coprime to n. In that case we impose an extra condition on s modulo g.

Now we address the following problem. Let A be a central simple $\mathbb{F}_q(t)$-algebra with a basis $b_1, \ldots, b_{n^2}$. Then one has that $b_i b_j = \sum_{k=1}^{n^2} \gamma_{ijk} b_k$, where $\gamma_{ijk} \in \mathbb{F}_q(t)$. The γ_{ijk} are called structure constants. We consider our algebra to be given as a collection of structure constants (i.e., we are given a multiplication table of its basis elements). We apply our previous algorithms to compute a primitive idempotent in a central simple $\mathbb{F}_q(t)$-algebra given by structure constants.

Theorem 1.12. *Let a central simple algebra A of degree n over $\mathbb{F}_q(t)$ be given by structure constants (where $\mathbb{F}_q$ contains the nth roots of unity). Then there exists a randomized polynomial time algorithm which constructs a primitive idempotent in A.*

Remark 1.13. First one computes the local Hasse invariants of A. The index of A is the least common multiple of the denominators of the nonzero Hasse invariants. Denote by m the index of A, Then we construct a symbol division algebra D with the same Hasse invariants. Then $A \otimes M_{\frac{n}{m}}(D)^{op}$ is isomorphic to a full matrix algebra over $\mathbb{F}_q(t)$. We construct an explicit isomorphism between the full matrix algebra and $A \otimes M_{\frac{n}{m}}(D)^{op}$ using the method from [5]. Finally, from such an isomorphism we construct the desired primitive idempotent.

Theorem 1.12 can also be applied when our algebra is given as a cyclic algebra, as structure constants can be computed in polynomial time from a cyclic algebra representation.

References

[1] G. Böckle, D. Gvírtz: Division algebras and maximal orders for given invariants; LMS Journal of Computation and Mathematics 19.A (2016): 178-195.
[2] J. Gómez-Torrecillas, F. J. Lobillo, G. Navarro: A new perspective of cyclicity in convolutional codes; IEEE Transactions on Information Theory 62.5 (2016): 2702-2706.
[3] J. Gómez-Torrecillas, F. J. Lobillo, G. Navarro: A Sugiyama-like decoding algorithm for convolutional codes; IEEE Transactions on Information Theory 63.10 (2017): 6216-6226.
[4] G. Ivanyos: Algorithms for algebras over global field; Ph. D. thesis, Hungarian Academy of Sciences, 1996.
[5] G. Ivanyos, P. Kutas, L. Rónyai: Computing explicit isomorphisms with full matrix algebras over $\mathbb{F}_q(x)$; Foundations of Computational Mathematics 18.2 (2018): 381-397.
[6] G. Ivanyos, P. Kutas, L. Rónyai: Explicit equivalence of quadratic forms over $\mathbb{F}_q(t)$; (2016) Preprint arXiv: arXiv:1610.08671.
[7] Reiner, Irving. Maximal orders. Vol. 5. Academic Pr, 1975.
[8] Serre, Jean-Pierre. Local fields. Vol. 67. Springer Science and Business Media, 2013.
[9] D. Wan: Generators and irreducible polynomials over finite fields; Mathematics of Computation 66.219 (1997), 1195-1212.

Institute for Computer Science and Control, Hungarian Academy of Sciences
E-mail address: kutasp@sztaki.hu

Monografías de la Real Academia de Ciencias. Zaragoza. **43:** 119–122, (2018).
ISSN: 1132-6360

LINEARIZED MULTIVARIATE SKEW POLYNOMIALS AND HILBERT 90 THEOREMS WITH MULTIVARIATE NORMS

UMBERTO MARTÍNEZ-PEÑAS

Abstract. We linearize the concept of free multivariate skew polynomials. We give a vector space description of their sets of roots in one conjugacy class, whose univariate counterpart is crucial in applications such as network coding. As a collateral consequence, we derive new Hilbert 90 theorems for general Galois field extensions. In contrast with the homological versions, these are computational theorems based on multivariate norms that reflect the relations among generators of the corresponding Galois group.

1. Introduction

Univariate skew polynomials were introduced by Ore in [6], and evaluation and interpolation using them were studied by Lam and Leroy in [1, 2]. Their results on linearizing their sets of roots are crucial for finding optimal error-correcting codes for the rank and sum-rank metrics [4], which have applications in linear network coding, among others (see [4] and its references). Moreover, they observed in [3] that Hilbert's famous Theorem 90 can be naturally written in terms of conjugacy and evaluation of skew polynomials.

In [5], we extended the concepts of skew polynomials and their evaluation and interpolation properties to free multivariate skew polynomial rings. One of the main motivations was to construct good codes for new (or old) metrics yet to be found. In this work, we give a linearized description of (free) multivariate skew polynomials and their root sets in one conjugacy class similar to that in [2]. We then deduce a generalization of Hilbert's Theorem 90 based on multivariate norms reflecting the relations among generators of the Galois group.

Throughout this paper, we will use the definitions, results and notations from [5]. Fix a division ring $\mathbb{F}$ and variables $x_1, x_2, \ldots, x_n$ and denote by $\mathcal{M}$ the set of (free) strings on these variables, which we will simply call monomials. Inspired by Ore's work [6], we showed in [5, Th. 1] that a product in a free multivariate polynomial ring with coefficients in $\mathbb{F}$ consists in appending monomials and is additive on degrees if, and only if, there exist a ring morphism $\sigma : \mathbb{F} \longrightarrow \mathbb{F}^{n\times n}$ and a σ-derivation $\delta : \mathbb{F} \longrightarrow \mathbb{F}^n$ such that

$$\mathbf{x}\beta = \sigma(\beta)\mathbf{x} + \delta(\beta),$$

for all $\beta \in \mathbb{F}$, where $\mathbf{x}$ is the column vector whose i-th component is x_i, for $i = 1, 2, \ldots, n$. We denote by $\mathbb{F}[\mathbf{x}; \sigma, \delta]$ such a non-commutative ring.

2. Linearized multivariate skew polynomials

We start by introducing linearized multivariate skew polynomials.

Definition 2.1. Given a (ring) morphism $\sigma : \mathbb{F} \longrightarrow \mathbb{F}^{n\times n}$, a σ-derivation $\delta : \mathbb{F} \longrightarrow \mathbb{F}^n$, a point $\mathbf{a} \in \mathbb{F}^n$ and a monomial $\mathfrak{m} \in \mathcal{M}$, we define the operator

$$\mathcal{D}_{\mathbf{a}}^{\mathfrak{m}} : \mathbb{F} \longrightarrow \mathbb{F}$$

as follows. First we define $\mathcal{D}_{\mathbf{a}}^{1} = \mathrm{Id}$, then we define

$$\mathcal{D}_{\mathbf{a}}(\beta) = (\mathcal{D}_{\mathbf{a}}^{x_1}(\beta), \mathcal{D}_{\mathbf{a}}^{x_2}(\beta), \ldots, \mathcal{D}_{\mathbf{a}}^{x_n}(\beta))^T = \sigma(\beta)\mathbf{a} + \delta(\beta) \in \mathbb{F}^n,$$

for all $\beta \in \mathbb{F}$. Next, if $\mathcal{D}_{\mathbf{a}}^{\mathfrak{m}}$ is defined for $\mathfrak{m} \in \mathcal{M}$, then we define

$$\mathcal{D}_{\mathbf{a}}^{\mathbf{x}\mathfrak{m}}(\beta) = (\mathcal{D}_{\mathbf{a}}^{x_1\mathfrak{m}}(\beta), \mathcal{D}_{\mathbf{a}}^{x_2\mathfrak{m}}(\beta), \ldots, \mathcal{D}_{\mathbf{a}}^{x_n\mathfrak{m}}(\beta))^T = \sigma(\mathcal{D}_{\mathbf{a}}^{\mathfrak{m}}(\beta))\mathbf{a} + \delta(\mathcal{D}_{\mathbf{a}}^{\mathfrak{m}}(\beta)) \in \mathbb{F}^n,$$

for all $\beta \in \mathbb{F}$. Denote by $\mathbb{F}[\mathcal{D}_{\mathbf{a}}]$ the left vector space over $\mathbb{F}$ with basis $\{\mathcal{D}_{\mathbf{a}}^{\mathfrak{m}} \mid \mathfrak{m} \in \mathcal{M}\}$. We define linearized multivariate skew polynomials as the elements of $\mathbb{F}[\mathcal{D}_{\mathbf{a}}]$. Given $F \in \mathbb{F}[\mathbf{x}; \sigma, \delta]$, we may construct a $F^{\mathcal{D}} \in \mathbb{F}[\mathcal{D}_{\mathbf{a}}]$ as the image of F by the left linear map

$$\begin{array}{ccc} \mathbb{F}[\mathbf{x}; \sigma, \delta] & \longrightarrow & \mathbb{F}[\mathcal{D}_{\mathbf{a}}] \\ \sum_{\mathfrak{m}\in\mathcal{M}} F_{\mathfrak{m}}\mathfrak{m} & \mapsto & \sum_{\mathfrak{m}\in\mathcal{M}} F_{\mathfrak{m}}\mathcal{D}_{\mathbf{a}}^{\mathfrak{m}}. \end{array}$$

Linearized skew polynomials are right linear over certain division subrings of $\mathbb{F}$, called centralizers, which motivates the terminology. Centralizers for univariate skew polynomials were defined in [2, Eq. (3.1)].

Definition 2.2. Given $\mathbf{a} \in \mathbb{F}^n$, we define its (σ, δ)-centralizer, or simply centralizer, as

$$K_{\mathbf{a}} = K_{\mathbf{a}}^{\sigma,\delta} = \{\beta \in \mathbb{F} \mid \mathcal{D}_{\mathbf{a}}(\beta) = \mathbf{a}\beta\}.$$

The following lemma extends [2, Lemma 3.2] (see also [3, Sec. 3]) from the univariate to the multivariate case. The proof is straightforward.

Lemma 2.3. *For all $\mathbf{a} \in \mathbb{F}^n$, it holds that $K_{\mathbf{a}} \subseteq \mathbb{F}$ is a division subring of $\mathbb{F}$. Moreover, for $F \in \mathbb{F}[\mathcal{D}_{\mathbf{a}}]$, the map $\beta \mapsto F(\beta)$, for $\beta \in \mathbb{F}$, is right linear over $K_{\mathbf{a}}$.*

We now connect multivariate skew polynomial evaluation [5, Def. 3] and linearized skew polynomial evaluation. The following result can be proven exactly as [4, App. A].

Theorem 2.4. *Given $\mathbf{a} \in \mathbb{F}^n$, $\beta \in \mathbb{F}^*$, $F \in \mathbb{F}[\mathbf{x}; \sigma, \delta]$, and writing $\mathcal{D} = \mathcal{D}_{\mathbf{a}}$, it holds that*

$$F(\mathcal{D}(\beta)\beta^{-1}) = F^{\mathcal{D}}(\beta)\beta^{-1}.$$

3. Linearized P-closed sets in one conjugacy class

In this section, we give linearized descriptions of finitely generated P-closed sets in one conjugacy class. Here, we will need the concepts of conjugacy, P-closed sets, P-independence and P-bases from [5]. We denote by $\overline{\mathcal{A}} = Z(I(\mathcal{A})) \subseteq \mathbb{F}^n$ the P-closure of a set $\mathcal{A} \subseteq \mathbb{F}^n$. Observe that the conjugacy relation in [5, Def. 4] is $\mathbf{a} \sim \mathbf{b}$ if, and only if, there exists $\beta \in \mathbb{F}^*$ such that $\mathbf{b} = \mathbf{a}^{\beta} = \mathcal{D}_{\mathbf{a}}(\beta)\beta^{-1}$. We will denote by $C(\mathbf{a})$ the conjugacy class of $\mathbf{a} \in \mathbb{F}^n$.

Our main result is the following lemma, which extends [2, Th. 4.5] from the univariate to the multivariate case.

Lemma 3.1. *Let $\mathbf{a}, \mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_M \in \mathbb{F}^n$ and $\beta_1, \beta_2, \ldots, \beta_M \in \mathbb{F}^*$ be such that*

$$\mathbf{b}_i = \mathcal{D}_{\mathbf{a}}(\beta_i)\beta_i^{-1},$$

for $i = 1, 2, \ldots, M$. Then $\mathcal{B} = \{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_M\}$ is P-independent if, and only if, $\mathcal{B}_{\mathcal{D}} = \{\beta_1, \beta_2, \ldots, \beta_M\}$ is right linearly independent over $K_{\mathbf{a}}$.

Proof. Assume first that $\mathcal{B}$ is P-independent, but $\mathcal{B}_\mathcal{D}$ is not right linearly independent over $K_\mathbf{a}$. Let $\mathcal{B}^* = \{F_1, F_2, \dots, F_M\} \subseteq \mathbb{F}[\mathbf{x}, \sigma, \delta]$ be a dual P-basis of $\mathcal{B}$ (see [5, Def. 11]). We may assume without loss of generality that there exist $\lambda_1, \lambda_2, \dots, \lambda_{M-1} \in K_\mathbf{a}$ such that

$$\beta_M = \sum_{i=1}^{M-1} \beta_i \lambda_i.$$

Therefore by Lemma 2.3 and Theorem 2.4, we reach the following contradiction

$$\beta_M = F_M^\mathcal{D}(\beta_M) = \sum_{i=1}^{M-1} F_M^\mathcal{D}(\beta_i)\lambda_i = 0.$$

Assume now that $\mathcal{B}_\mathcal{D}$ is right linearly independent over $K_\mathbf{a}$. We will prove by induction on M that $\mathcal{B}$ is P-independent. The case $M = 1$ is obvious since singleton sets are always P-independent. Assume then that $\mathcal{B}' = \{\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_{M-1}\}$ is P-independent but $\mathbf{b}_M \in \overline{\mathcal{B}'}$.

First we see that we may assume without loss of generality that $\beta_M = 1$, redefining $\beta_i = \beta_i \beta_M^{-1}$ and $\mathbf{a} = \mathbf{b}_M$ ($\mathbf{b}_i$ remains unchanged), for $i = 1, 2, \dots, M$.

Now let $\mathcal{B}'^* = \{F_1, F_2, \dots, F_{M-1}\}$ be a dual P-basis of $\mathcal{B}'$. Fix $i = 1, 2, \dots, M-1$ and define $\mathbf{G}_i = (\mathbf{x} - \mathbf{b}_i)F_i \in \mathbb{F}[\mathbf{x}; \sigma, \delta]^n$. It holds that $\mathbf{G}_i(\mathbf{b}_j) = \mathbf{0}$, for $j = 1, 2, \dots, M-1$, by [5, Th. 3]. Since $\mathbf{a} = \mathbf{b}_M \in \overline{\mathcal{B}'}$, we deduce from [5, Th. 3] and [5, Th. 5] that

$$\mathbf{0} = \mathbf{G}_i(\mathbf{a}) = (\mathbf{a}^{F_i(\mathbf{a})} - \mathbf{b}_i)F_i(\mathbf{a}) = \mathcal{D}_\mathbf{a}(F_i(\mathbf{a})) - \mathcal{D}_\mathbf{a}(\beta_i)\beta_i^{-1}F_i(\mathbf{a})$$

if $F_i(\mathbf{a}) \neq 0$. Now, we have that

$$\mathcal{D}_\mathbf{a}(F_i(\mathbf{a}))F_i(\mathbf{a})^{-1} = \mathcal{D}_\mathbf{a}(\beta_i)\beta_i^{-1} \iff \mathbf{a}^{F_i(\mathbf{a})} = \mathbf{a}^{\beta_i} \iff \mathbf{a}^{\beta_i^{-1}F_i(\mathbf{a})} = \mathbf{a},$$

thus $\beta_i^{-1}F_i(\mathbf{a}) \in K_\mathbf{a}$. Hence in all cases ($F_i(\mathbf{a}) = 0$ or $\neq 0$) we have that $F_i(\mathbf{a}) = \beta_i\lambda_i$, for some $\lambda_i \in K_\mathbf{a}$. Next if $F = F_1 + F_2 + \cdots + F_{M-1}$, we have that $F(\mathbf{b}_j) = 1$, for $j = 1, 2, \dots, M-1$. Since $\mathbf{a} = \mathbf{b}_M \in \overline{\mathcal{B}'}$, we deduce from [5, Th. 5] the following contradiction

$$\beta_M = 1 = F(\mathbf{a}) = \sum_{i=1}^{M-1} F_i(\mathbf{a}) = \sum_{i=1}^{M-1} \beta_i\lambda_i.$$

□

With the same techniques, we can also prove that if $\mathcal{G} \subseteq \mathbb{F}^n$ is finite and $\mathbf{b} \in \overline{\mathcal{G}}$, then $\mathbf{b}$ is conjugate to an element in $\mathcal{G}$. Hence we can easily deduce the following result.

Theorem 3.2. *Let $\mathbf{a} \in \mathbb{F}$. The following hold:*

(1) *If $\mathcal{G} \subseteq C(\mathbf{a})$ is finite and $\Omega = \overline{\mathcal{G}} \subseteq \mathbb{F}^n$, then*

$$\Omega = \{\mathcal{D}_\mathbf{a}(\beta)\beta^{-1} \mid \beta \in \Omega^\mathcal{D} \setminus \{0\}\} \subseteq C(\mathbf{a}), \tag{1}$$

for a finite-dimensional right vector space $\Omega^\mathcal{D} \subseteq \mathbb{F}$ over $K_\mathbf{a}$.

(2) *Conversely, if $\Omega^\mathcal{D} \subseteq \mathbb{F}$ is a finite-dimensional right vector space over $K_\mathbf{a}$, then $\Omega \subseteq C(\mathbf{a})$ given as in (1) is a finitely generated P-closed set.*

Moreover if Item 1 or 2 holds, then $\mathcal{B}$ is a P-basis of Ω if, and only if, $\mathcal{B}_\mathcal{D} = \{\beta \in \mathbb{F}^* \mid \mathcal{D}_\mathbf{a}(\beta)\beta^{-1} \in \mathcal{B}\}$ is a right basis of $\Omega^\mathcal{D}$ over $K_\mathbf{a}$. In particular, we have that

$$\mathrm{Rk}(\Omega) = \dim_{K_\mathbf{a}}(\Omega^\mathcal{D}).$$

The following important consequence follows immediately:

Corollary 3.3. *Let $\mathbf{a} \in \mathbb{F}^n$. The conjugacy class $C(\mathbf{a}) \subseteq \mathbb{F}^n$ is P-closed and finitely generated if, and only if, $\mathbb{F}$ is a finite-dimensional right vector space over $K_{\mathbf{a}}$.*

4. Hilbert 90 theorems with multivariate norms

As observed in [3], generalizations of Hilbert's Theorem 90 can be understood as any effective criterion for conjugacy. Thus we can give a general statement from Corollary 3.3.

Theorem 4.1 (**Multivariate Hilbert 90**). *Let $\mathbf{a} \in \mathbb{F}^n$, assume that $\mathbb{F}$ is a finite-dimensional right vector space over $K_{\mathbf{a}}$, and let $\{F_j\}_{j\in J}$ be generators of $I(C(\mathbf{a}))$ as a left ideal. For $\mathbf{b} \in \mathbb{F}^n$, there exists $\beta \in \mathbb{F}^*$ such that*

$$\mathbf{b} = \mathcal{D}_{\mathbf{a}}(\beta)\beta^{-1},$$

if and only if, $F_j(\mathbf{b}) = 0$, for all $j \in J$, where evaluation is as in [5, Def. 3].

Assume now that $\mathbb{F}$ is a field, $\mathbf{a} = \mathbf{1} = (1, 1, \ldots, 1)$, $\delta = 0$ and $\sigma = \operatorname{diag}(\sigma_1, \sigma_2, \ldots, \sigma_n)$, for field automorphisms $\sigma_i : \mathbb{F} \longrightarrow \mathbb{F}$, for $i = 1, 2, \ldots, n$ (as in [5, Ex. 1]). Then $K = K_{\mathbf{1}} = \mathbb{F}^G$ is the field of invariant elements of $\mathbb{F}$ by the group G generated by $\sigma_1, \sigma_2, \ldots, \sigma_n$. If G is finite and $K \subseteq \mathbb{F}$ is a Galois extension, we can easily prove, using Theorem 2.4, that the set

$$\{\mathfrak{m} - \mathfrak{n} \in \mathbb{F}[\mathbf{x}; \sigma, \delta] \mid \mathfrak{m}, \mathfrak{n} \in \mathcal{M}, \mathfrak{m}(\sigma) = \mathfrak{n}(\sigma)\}$$

generates $I(C(\mathbf{1}))$, where $\mathfrak{m}(\sigma)$ is the conventional symbolic evaluation of $\mathfrak{m}$ in $(\sigma_1, \sigma_2, \ldots, \sigma_n)$. Thus we deduce the following generalization of Hilbert 90 for Galois field extensions.

Corollary 4.2. *Let $K \subseteq \mathbb{F}$ be a Galois extension of fields with Galois group G generated by $\sigma_1, \sigma_2, \ldots, \sigma_n$. For a list $\mathbf{b} = (b_1, b_2, \ldots, b_n) \in (\mathbb{F}^*)^n$, there exists $\beta \in \mathbb{F}^*$ such that*

$$b_i = \sigma_i(\beta)\beta^{-1}, \quad \text{for all } i = 1, 2, \ldots, n,$$

if and only if, the following equations are satisfied:

$$N_{\mathfrak{m}}(\mathbf{b}) = N_{\mathfrak{n}}(\mathbf{b}), \quad \text{whenever } \mathfrak{m}(\sigma) = \mathfrak{n}(\sigma),$$

where $N_{\mathfrak{m}}(\mathbf{b}) = \mathfrak{m}(\mathbf{b})$ and $N_{\mathfrak{n}}(\mathbf{b}) = \mathfrak{n}(\mathbf{b})$ can be computed recursively as in [5, Th. 2].

Acknowledgement: This work is supported by The Independent Research Fund Denmark under Grant No. DFF-7027-00053B.

References

[1] T. Y. Lam. A general theory of Vandermonde matrices. *Expositiones Mathematicae*, 4:193–215, 1986.
[2] T. Y. Lam and A. Leroy. Vandermonde and Wronskian matrices over division rings. *Journal of Algebra*, 119(2):308–336, 1988.
[3] T. Y. Lam and A. Leroy. Hilbert 90 theorems over divison rings. *Transactions of the American Mathematical Society*, 345(2):595–622, 1994.
[4] U. Martínez-Peñas. Skew and linearized Reed-Solomon codes and maximum sum rank distance codes over any division ring. *Journal of Algebra* (In press), 2018.
[5] U. Martínez-Peñas and F. R. Kschischang. Evaluation and interpolation over multivariate skew polynomial rings. pages 1–28, 2017. Submitted. Available: `https://arxiv.org/abs/1710.09606`.
[6] O. Ore. Theory of non-commutative polynomials. *Annals of Mathematics (2)*, 34(3):480–508, 1933.

Dept. of Electrical & Computer Engineering, University of Toronto, Canada
E-mail address: `umberto@math.aau.dk`

Monografías de la Real Academia de Ciencias. Zaragoza. **43:** 123–126, (2018).
ISSN: 1132-6360

COPOLAR AND NON-COPOLAR PROPERTIES OF MONOMIAL IDEALS

F. MOHAMMADI, P. PASCUAL-ORTIGOSA, AND E. SÁENZ-DE-CABEZÓN

Abstract. Monomial ideals that have the same polarization are called copolar. Copolar ideals share several important properties, like Betti numbers or height. Given an ideal I we can obtain information about it by examining the family of ideals copolar to a it. We give some examples of this approach that demonstrate its utility.

1. Polarity classes

Polarization is a well known operation that transforms a monomial ideal into a squarefree monomial ideal that shares several important properties with the original one [2, 4, 5]. Conversely, depolarization is the operation that given a squarefree ideal I gives a monomial ideal J such that I is its polarization. We say that two monomial ideals are in the same polarity class i.e. are *copolar* if they have the same polarization. In [8] the authors introduce the concepts of *support poset* and *depolarization poset* and give a method to find all the ideals that have the same polarization. The main definitions and results in [8] are the following.

Definition 1.1. Let $n \in \mathbb{N}$ and let $(a_1, \ldots, a_n) \in \mathbb{N}^n$. Let $\mu = (b_1, \ldots, b_n) \in \mathbb{N}^n$ where $b_i \leq a_i$ for all i. The polarization of μ in $\mathbb{N}^{a_1+\cdots+a_n}$ is the multi-index $\overline{\mu} = (\overbrace{1, \ldots, 1}^{b_1}, \overbrace{0, \ldots, 0}^{a_1-b_1}, \ldots, \overbrace{1, \ldots, 1}^{b_n}, \overbrace{0, \ldots, 0}^{a_n-b_n})$. The *polarization of* $\mathbf{x}^{\mu} = x_1^{b_1} \cdots x_n^{b_n} \in R = \mathbf{k}[x_1, \ldots, x_n]$ is the squarefree monomial $\mathbf{x}^{\overline{\mu}} = x_{1,1} \cdots x_{1,b_1} \cdots x_{n,1} \cdots x_{n,b_n}$ in $S = \mathbf{k}[x_{1,1}, \ldots, x_{1,a_1}, \ldots, x_{n,1}, \ldots, x_{n,a_n}]$ (observe that for ease of notation we used $\mathbf{x}$ with two different meanings in this definition).

Let $I = \langle m_1, \ldots, m_r \rangle$ be a monomial ideal in $R = \mathbf{k}[x_1, \ldots, x_n]$. The *polarization of* I, denoted by $\overline{I}$, is the monomial ideal in $S = \mathbf{k}[x_{1,1}, \ldots, x_{1,a_1}, \ldots, x_{n,1}, \ldots, x_{n,a_n}]$ given by $\overline{I} = \langle \overline{m_1}, \ldots, \overline{m_r} \rangle$, where a_i is the maximum exponent to which indeterminate x_i appears among the monomials in $G(I)$.

Let $I \subseteq R$ be a squarefree monomial ideal. A *depolarization of* I is a monomial ideal $J \subseteq S$ such that I is equivalent to $\overline{J} \subseteq T$ i.e. R and T have the same number of variables and there is a bijective map φ from the set of variables of R to the set of variables of T such that $\varphi(G(I)) = G(J)$, where $G(J)$ is the unique minimal monomial generating set of J.

Let $I \subseteq R = \mathbf{k}[x_1, \ldots, x_n]$ be a squarefree monomial ideal. Let $G(I) = \{m_1, \ldots, m_r\}$ be the unique minimal monomial generating set of I. For each x_i, $1 \leq i \leq n$ the set $C_i \subseteq \{x_1, \ldots, x_n\}$ is given by the indices of all the variables that appear in every minimal generator of I in which x_i is present, including x_i itself. Let C_I be the set of the C_i's just defined. The poset on the elements of C_I ordered by inclusion is called the *support poset* of

I and is denoted suppPos(I). The *support poset* of a general monomial ideal is the support poset of its polarization.

The support poset of any monomial ideal $I \subseteq R = \mathbf{k}[x_1, \ldots, x_n]$, together with a given ordering $<$ on the variables $x_1, \ldots, x_n$ induces a partial order $\prec$ in the set of variables as follows: $x_i \prec x_j$ if $C_i \subset C_j$ or if $C_i = C_j$ and $x_i < x_j$. This poset is the $<$*-support poset* of I denoted suppPos$_<(I)$.

Not every poset is the support poset of a monomial ideal. We can however give some conditions on the poset, like the following result.

Proposition 1.2. *Let P be a directed forest. Then there is a monomial ideal I such that P is its support poset.*

Definition 1.3. Let $I \subseteq \mathbf{k}[x_1, \ldots, x_n]$ be a squarefree monomial ideal and $<$ a total order on the variables. A *depolarization order* for I is a partition of suppPos$_<(I)$ in disjoint paths.

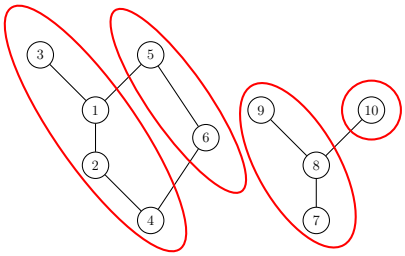
Using any depolarization order of a squarefree monomial ideal I, we can construct a depolarization of I. Let $(\overline{P}, <)$ be a depolarization order for a squarefree monomial ideal $I \subseteq R = \mathbf{k}[x_1, \ldots, x_n]$, where $\overline{P} = \{\sigma_1, \ldots, \sigma_k\}$ and each σ_i is a path in suppPos(I). We construct a depolarization J of I in a polynomial ring $S = \mathbf{k}[y_1, \ldots, y_k]$ as follows: for each $m \in G(I)$ consider the monomial m' given by the image of m under the correspondence $x_i \mapsto y_j$ for each $i \in \sigma_j$. This produces a monomial ideal J whose polarization $\overline{J}$ is clearly equivalent to I with the map sending $y_{j,l} \mapsto x_{\sigma_{j_l}}$ where σ_{j_l} is the l'th element of σ_j under the order $<$. Every depolarization is obtained in this way.

Theorem 1.4. *Let $I = \langle m_1, \ldots, m_r \rangle \subseteq R = \mathbf{k}[x_1, \ldots, x_n]$ be a squarefree monomial ideal. Every depolarization of I can be obtained from a depolarization order of I.*

Example 1.5. Let I be the squarefree monomial ideal

$$I = \langle x_1x_2x_3x_4, x_4x_6x_7, x_1x_2x_4x_5x_6, x_7x_8x_9, x_7x_8x_{10} \rangle \subseteq \mathbf{k}[x_1, \ldots, x_{10}].$$

The figure shows a path partition of its support poset with respect to any order of the variables such that $x_2 < x_1$. It gives the depolarization $J = \langle y_1^4, y_1y_2y_3, y_1^3y_2^2, y_3^3, y_3^2y_4 \rangle \subseteq \mathbf{k}[y_1, y_2, y_3, y_4]$ for I. The equivalence between $\overline{J}$ and I is given by $y_{1,1} \mapsto x_4$, $y_{1,2} \mapsto x_2$, $y_{1,3} \mapsto x_1$, $y_{1,4} \mapsto x_3$, $y_{2,1} \mapsto x_6$, $y_{2,2} \mapsto x_5$, $y_{3,1} \mapsto x_7$, $y_{3,2} \mapsto x_8$, $y_{3,3} \mapsto x_9$, $y_{4,1} \mapsto x_{10}$.



The set of all path partitions of a given poset are sorted by refinement and using this ordering they form themselves a poset. Let I be a squarefree monomial ideal and let J and J' be two depolarizations of I. We say that $J \leq J'$ if the path partition giving rise to J is

a refinement of the one corresponding to J'. The set of ideals that are a depolarization of a given squarefree monomial ideal I forms a poset in which I is the unique minimal element. We call this the *depolarization poset* of I, denoted $\mathrm{DP}(I)$. Given any monomial ideal J, we say that the *depolarization poset* of J is the depolarization poset of its polarization J', i.e. $\mathrm{DP}(J) \equiv \mathrm{DP}(J')$.

Definition 1.6. We say that two monomial ideals I and J are *copolar* if their polarizations are equivalent i.e., if they are in the same depolarization poset.

2. Copolar properties

Let $\mathrm{lcm}(I)$ be the least common multiple lattice of I, cf. [3].

Lemma 2.1. *Let I and J two copolar ideals, then* $\mathrm{lcm}(I) \cong \mathrm{lcm}(J)$.

Hence, any property that depends on the lcm-lattice is copolar i.e. is the same for copolar ideals. The lcm-lattice of a monomial ideal encodes the structure of its minimal free resolution and thus its Betti numbers [3] and all related invariants, like regularity or projective dimension. Some other important invariants are also fixed under polarization. The following is a list of copolar properties (cf. [4, 2]).

Proposition 2.2. *Let $I \subseteq S$ be a monomial ideal and $J \subseteq T$ its polarization. Then*

1. $\beta_{i,j}(I) = \beta_{i,j}(J)$ *for all i and j;*
2. $H_I(t) = (1-t)^{\delta} H_J(t)$ *where* $\delta = \dim T - \dim S$*;*
3. $\mathrm{height}(I) = \mathrm{height}(J)$*;*
4. $\mathrm{projdim}(S/I) = \mathrm{projdim}(T/J)$ *and* $\mathrm{reg}(S/I) = \mathrm{reg}(T/J)$*;*
5. *S/I is Cohen-Macaulay (resp. Gorenstein) if and only if T/J is Cohen-Macaulay (resp. Gorenstein).*

Other recent results in this direction show that the Stanley conjecture can be reduced to the squarefree case via polarization, and that the Stanley projective dimension is invariant under polarization [6, 7].

3. Using depolarization to relate copolar and non-copolar properties

The fact that some properties are copolar and some convenient ones are not gives us a way to use the latter to obtain information about ideals. The general procedure is the following: explore the depolarization lattice of a monomial ideal to find a special ideal with some particular property that has consequences that can then be applied to all its copolarity class.

A good example of this is that quasi-stable monomial ideals (also known as nested-type) have some nice properties that allow us to compute their regularity, projective dimension and finding a free resolution cf. [9, 10, 1]. Finding a quasi-stable ideal in the depolarization poset allows us to compute the regularity and projective dimension of all ideals in its polarity class. In particular, zero-dimensional ideals are quasi-stable, hence the following two propositions provide an example of the above procedure:

Proposition 3.1. *Let $(P, \subseteq)$ be a poset of subsets of the set $[nm]$ formed by $n > 1$ disjoint paths each of length m. Then there is at least one squarefree monomial ideal $I_{n,m}$ such that P is its support poset and there is a zero-dimensional monomial ideal $J_{n,m}$ copolar to $I_{n,m}$.*

Proposition 3.2. *Let n be a positive integer and $m_1, \ldots, m_n$ positive integers such that $m_i \leq n$ for all n. Let $m = \sum_i m_i$ and let $(P, \prec)$ a poset of subsets of the set $[m]$ formed by n disjoint paths each of length m_i. Then there is at least one squarefree monomial ideal I such that P is its support poset except if $n = 2$ and $m_1 \neq m_2$. Moreover, if for all i $m_i > 1$, then there is a zero-dimensional monomial ideal copolar to I.*

The next proposition is an example of the same procedure in which we find an ideal in a polarity class of which we are able to compute the homological invariants that can be transferred to all ideals copolar to it.

Proposition 3.3. *Let $(P, \subseteq)$ be a poset of subsets of the set $[4m]$ formed by $m \geq 1$ disjoint diamonds $D_1, \ldots, D_m$, $D_i = \{a_{i1}, \ldots, a_{i4}\}$ with $a_{i1} < a_{i2}$, $a_{i1} < a_{i3}$, $a_{i2} < a_{i4}$, $a_{i3} < a_{i4}$. Then there is at least one squarefree monomial ideal I_m such that P is its support poset and for every ideal J_m in its polarity class we have $\operatorname{reg}(J_m) = 2m$ and $\operatorname{projdim}(J_m) = \lfloor \frac{m}{2} \rfloor$ and its minimal free resolution is given as an iterated cone resolution.*

References

[1] I. Bermejo and P. Gimenez, *Saturation and Castelnuovo-Mumford regularity*, Journal of Algebra, vol. 303, 2006, pp. 592-617.

[2] S. Faridi, *Monomial ideals via squarefree monomial ideals*, arXiv preprint arXiv:math/0507238v1

[3] V. Gasharov, I. Peeva and V. Welker, *The lcm-lattice in monomial resolutions*, Mathematical Research Letters 6, 1999, pp. 521-532

[4] J. Herzog and T. Hibi, *Monomial Ideals*, Graduate Texts in Mathematics 260, Springer, London, 2010.

[5] J. Herzog, T. Hibi and A.A. Qureshi, *Polarization of Koszul cycles with applications to powers of edge ideals of whisker graphs*, Proceedings of the American Mathematical Society 143(7), 2015, pp. 2767–2778.

[6] B. Ichim, L. Katthän and J.J. Moyano-Fernández, *The behavior of Stanley depth under polarization*, J. Combin. Theory ser. A, 135, 2015, pp. 332–347

[7] B. Ichim, L. Katthän and J.J. Moyano-Fernández, *Stanley depth and the lcm-lattice*, J. Combin. Theory ser. A, 150, 2017, pp. 295–322

[8] F.Mohammadi, P. Pascual-Ortigosa, E. Sáenz-de-Cabezón, H. Wynn, *Polarization and depolarization of monomial ideals with application to multi-state system reliability*, submitted 2018

[9] W.M. Seiler, *A combinatorial approach to involution and delta-regularity I: involutive bases in polynomial algebras of solvable type*, Applicable Algebra Eng. Commun. Comput., vol. 20, 2009, pp. 207–259.

[10] W.M. Seiler, *A combinatorial approach to involution and delta-regularity II: structure analysis of polynomial modules with Pommaret bases*, Applicable Algebra Eng. Commun. Comput., vol. 20, 2009, pp. 261–338.

School of Mathematics, University of Bristol
E-mail address: fatemeh.mohammadi@bristol.ac.uk

Universidad de La Rioja
E-mail address: papasco@unirioja.es

Universidad de La Rioja
E-mail address: eduardo.saenz-de-cabezon@unirioja.es

Monografías de la Real Academia de Ciencias. Zaragoza. **43:** 127–130, (2018).
ISSN: 1132-6360

AUTOMATIC DEDUCTION OF GEOMETRIC THEOREMS USING THE GRÖBNER COVER

ANTONIO MONTES

Abstract. We have developed an automatic algorithm for obtaining the supplementary conditions for a proposition to become a theorem. It has been implemented in the Singular library "grobcov.lib". We give here an approach to it.

Introduction

Consider a geometric proposition of the form

$$(H \wedge \neg H_1) \Rightarrow (T \wedge \neg T_1). \tag{1}$$

We are interested in obtaining supplementary conditions for Proposition (1) to become a theorem. In this kind of problem, we assume that there are a set of *free variables* $\mathbf{u} = u_1, \dots u_n$ of the geometric construction, that we take as *parameters*, and a set of *dependent variables* $\mathbf{v} = v_1, \dots, v_m$, that we take as variables. The problem is a special kind of geometrical locus problem: for which values of the parameters Proposition (1) is true.

We work in the ring $R = \mathbb{C}[\mathbf{u}][\mathbf{v}]$ and use the Gröbner Cover [3], that provides the canonical discussion of a parametric ideal. We assume that H, H_1, T, T_1 are parametric ideals, being the negative hypothesis H_1 described by an ideal in the parameters.

The Singular command $G =$`grobcov`(F), where F is a parametric ideal in $R = \mathbb{C}[\mathbf{u}][\mathbf{v}]$ to be discussed, outputs a list G of segments $G_i = [\mathrm{lpp}_i, B_i, S_i]$. The S_i are locally closed subsets of the parameter space described in P or C-representation depending on the option `"rep"`,(0,1). B_i is the corresponding basis that specializes to the reduced Gröbner basis of F on the segment S_i, and lpp_i is the set of leading power products of the basis B_i, as well as of the specialized Gröbner basis for every fixed values of the parameters.

The algorithm ADGT uses grobcov, and automatically returns the complementary conditions on the parameters for Proposition (1) to become a theorem. It is completely described in the book [1] that will properly be published in the ACM Springer collection.

1. Algorithm ADGT

Consider first a geometric statement of the form

$$H \wedge \neg H_1 \Rightarrow T. \tag{2}$$

The `grobcov` command allows as options `"null"`,E and `"nonnull"`,N, where E, N are ideals in the parameters, and whose effect is restricting the parameter space to be analyzed to $\mathbf{V}(E) \setminus \mathbf{V}(N)$. We have to determine the values of the parameters for which the ideal $H + T$ has solutions, restricting the parameter space to $\mathbf{V}(0) \setminus \mathbf{V}(H_1)$. Algorithm 2:

ADGT (Automatic Deduction of Geometric Theorem) does it on line 1, where it uses options `"nonnull"`,H_1 to restrict the parameter space to the values $\mathbf{V}(0)\setminus\mathbf{V}(H_1)$ and `"rep",1`, for obtaining the segments in C-representation.

Let $J=\{i_1,\ldots,i_t\}$ be the set of indices of the segments S_i of G with lpp $\neq\{1\}$, i.e. the indices of the segments where the system $H+T$ has solutions. Then, the necessary and sufficient complementary hypothesis for statement (2) to hold is the set of the parameter values in $S=\bigcup_{i\in J}S_i$. We can read the conditions directly in G. In that case, we can obtain further information, and distinguish between points with a single solution, with a finite number of solutions or with infinitely many solutions. This can be useful for a deep analysis of the problem, but here we are interested in obtaining uniquely the necessary and sufficient conditions in an automatic way.

We can summarize the conditions, representing a constructible set S, determining the levels L of S by applying Algorithm 1: CompLev to G.

$L\leftarrow$ **CompLev**(G)
`Input`:
  $G=$ the `grobcov` of a proposition in C-representation
`Output`:
  $L=[I_1,I_2,\ldots,I_k]$: the levels of the constructible set S
    of supplementary conditions.
begin
  $S=$ Select the segments S_i of G for which lpp $\neq\{1\}$
  $L=$ `ConsLevels`(S)
  return(L)
end

Algorithm 1: `CompLev`

The procedure CompLev will first select the segments S_i of G for which lpp $\neq\{1\}$, and will return a list of pairs $[E_i,N_i]$ representing (in C-representation) the sets $\mathbf{V}(E_i)\setminus\mathbf{V}(N_i)$ where the system defined in G has solutions. We will have $S=(\mathbf{V}(E_1)\setminus\mathbf{V}(N_1))\cup\cdots\cup(\mathbf{V}(E_r)\setminus\mathbf{V}(N_r))$. Then ConsLevels constructs the canonical levels $I_1,\ldots,I_k$ of the constructible set S, (see [2]), being

$$I_1\subset I_2\subset\cdots\subset I_k$$
$$\overline{S}=\mathbf{V}(I_1)\supset\mathbf{V}(I_2)\supset\cdots\supset\mathbf{V}(I_k)=\emptyset,$$
$$\dim(S)=\dim(I_1)>\dim(I_2)>\ \ldots\ >\dim(I_k)=-1.$$
$$S=\bigcup_{i=1}^{k}\mathbf{V}(I_{2i-1})\setminus\mathbf{V}(I_{2i}).$$

In many problems, S is simply a variety $\mathbf{V}(I_1)$ or at most a locally closed set $\mathbf{V}(I_1)\setminus\mathbf{V}(I_2)$, because the set S is not only constructible, but also locally closed.

Now let us describe Algorithm 2: ADGT.

Lines 1,2 considers the case where no nonnull thesis is present, i.e. when $T_1=1$. It suffices to do as we have already described.

Then it considers the complete Proposition (1) for $T_1 \neq 1$.

To tackle Proposition (1) consider first a previous problem. Determine the complementary conditions for the statement $H \Rightarrow T_1$. For this purpose ADGT proceeds on lines 4,5 as before and obtains the levels of G_1.

$L \leftarrow$ **ADGT**$(H, T, H_1, T_1,$ `"options"`$)$
`Input`:
Ideals H, T, H_1, T_1
`Output`:
$L = [[1, [A_1, A_2], [2, [A_3, A_4]]..]$: the complementary conditions over the parameters, that must be added to H in order that the proposition $(H \wedge \neg H_1) \Rightarrow (T \wedge \neg T_1)$ becomes true
begin
1. **if** $T_1 = \langle 1 \rangle$ **then**
2. $G_2 =$ `grobcov`$(H + T,$ `"nonnull"`$, H_1,$ `"rep"`$, 1)$
3. **else**
4. $G_1 =$ `grobcov`$(H + T_1,$ `"rep"`$, 1)$
5. $L_1 =$ `CompLev`(G_1)
6. **for** all even i of L_1 **do** $L_1[i] = L_1[i] \cap H_1$ **end for**
7. $G_2 =$ `grobcov`$(H + T,$ `"nonnull"`$, L_1[1],$ `"rep"`$, 1)$
8. $m = \#L_0$; $r = \text{quot}(m, 2)$; **if** m is even **then** $r = r - 1$ **end if**
9. **for** $i = 1..r$ **do**
10. $G_3 =$ `grobcov`$(H + T,$ `"null"`$, L_1[2i],$ `"nonnull"`$, L_0[2i + 1],$ `"rep"`$, 1)$
11. $G_2 = G_2 \cup G_3$
12. **end for**
13. **end if**
14. $L =$ `Levels(CompLev`$(G_2))$
15. By default transform L to P-representation
16. **return**(L)
end

Algorithm 2: ADGT

Let S_1 be the segments of G_1 with solutions different from $\{1\}$, and L_1 its canonical levels. Then, $S_1 \cup \mathbf{V}(H_1)$ must be subtracted. First, on line 6 it computes the intersection of H_1 with the odd levels of G_1.

Then, beginning in line 7, ADGT determines G_2, where the first level $L_1[1]$ is subtracted from the complementary segments of the proposition $H \Rightarrow T$. But if there are more levels in L_1 this first subtraction has subtracted to many segments and thus it must add all the segments of the complement of S_1. This is done determining all the G_3, on lines 8 to 12, and add them together on line 11.

Finally, on line 14, it constructs the true levels of the complete set of segments:

All these steps are described in Algorithm 2: ADGT. In the implemented version, the command `ADGT` by default transforms the C-representation of the levels into their P-representation, as it is more illustrative. But, with option `"rep",1` this is avoided.

2. Examples

We show now some simple examples applying `ADGT`. We consider different propositions concerning the ortic triangle. Let $A(-1,0)$, $B(1,0)$, $C(x,y)$ be the coordinates of the triangle ABC. We want to determine the allowed positions of C in order to obtain the necessary and sufficient conditions for complementing two different "Propositions" related with the ortic triangle to convert them into "Theorems". Let $A'(x_1,y_1)$, $B'(x_2,y_2)$, $C'(x,0)$ be the foots of the heights, traced from A,B,C. The ortic triangle of ABC is $A'B'C'$.

Consider the following ideals of hypothesis and thesis:

Hypothesis H: The triangle $A'B'C'$ is the ortic triangle of ABC

$$H = -yx_1 + (x-1)y_1 + y,\ (x-1)(x_1+1) + yy_1,$$
$$-yx_2 + (x+1)y_2 - y,\ (x+1)(x_2-1) + yy_2;$$

Hypothesis H_1. The triangle ABC is degenerate (we shall deny it): $H_1 = y$;

Thesis T. The ortic triangle $A'B'C'$ is isosceles ($\overline{A'C'} = \overline{B'C'}$):

$$T = (x_1-x)^2 + y_1^2 - (x_2-x)^2 - y_2^2;$$

Thesis T_1. The ortic triangle $A'B'C'$ is degenerate (points aligned, we shall deny it):

$$T_1 = x(y_1-y_2) - y(x_1-x_2) + x_1y_2 - x_2y_1;$$

Proposition 1. $H \Rightarrow T$.

Calling sequence: `ADGT`$(H,T,1,1)$; Result:

$$(x,y) \in (\mathbf{V}(x^2-y^2-1) \setminus \mathbf{V}(y^2+1,x)) \cup (\mathbf{V}(x^2+y^2-1)) \cup (\mathbf{V}(x) \setminus \mathbf{V}(y^2+1,x))$$

We see that the supplementary conditions for Proposition 1 to be a Theorem are that the point C must be 1) either in the hyperbola $x^2-y^2-1=0$ except two complex points, 2) either on the circle $x^2+y^2-1=0$, 3) either on the mediatrix of segment AB except two complex points.

Case 1) is interesting. Case 2) corresponds to rectangular triangles whose ortic triangle is isosceles. Case 3) corresponds to ABC being isosceles itself.

Proposition 2. $H \wedge \neg H_1 \Rightarrow T \wedge \neg T_1$. Calling sequence: `ADGT`$(H,T,H_1,T_1)$; Result:

$$(x,y) \in (\mathbf{V}(x^2-y^2-1) \setminus (\mathbf{V}(y,x-1) \cup \mathbf{V}(y,x+1) \cup \mathbf{V}(y^2+1,x)))$$
$$\cup (\mathbf{V}(x) \setminus (\mathbf{V}(x,y) \cup \mathbf{V}(y^2+1,x)))$$

We see that denying the ortic triangle to be degenerate, eliminates case 2) of Prop. 1 as the rectangular triangles have degenerate ortic triangle. At the same time, denying ABC to be degenerate, eliminates points A, B and $(0,0)$, for which ABC is degenerate.

References

[1] A. Montes, The Gröbner Cover, ACM series, Springer, Berlin, Heidelberg, New York, (2018).
[2] J.M. Brunat, A. Montes, Computing the Canonical Representation of Constructible sets, International Journal of Mathematics in Computer Science, 10, (2016), 165–178.
[3] A. Montes, M. Wibmer, Gröbner bases for polynomial systems with parameters, J. Symbolic Comput., 45, (2010), 1391–1425.

Dep. Matemàtica Aplicada. Universitat Politècnica de Catalunya. Spain
E-mail address: antonio.montes@upc.edu

Monografías de la Real Academia de Ciencias. Zaragoza. **43:** 131–134, (2018).
ISSN: 1132-6360

ALGEBRAIC ANALYSIS OF MULTISTATE k-OUT-OF-n SYSTEMS

P. PASCUAL-ORTIGOSA, E. SÁENZ-DE-CABEZÓN, AND H. P. WYNN

Abstract. k-out-of-n systems have been intensively studied because of their importance in engineering and biology. In this paper we study the algebraic approach to their multistate version. We review the different definitions that multistate k-out-of-n systems have received and show how the algebraic method is used to study their reliability in a general way with a single approach.

Introduction

The study of the reliability of a system, i.e. the probability that the system works, is a relevant branch of engineering and network science. In this context we define binary systems with binary components as those in which both the system and each of the components can only be in two possible states: fail or work. An important class of binary systems are k-out-of-n systems, which have n components and work if and only if at least k of the components are working. For a detailed study of k-out-of-n systems see [6]. In practice, binary systems are unable to model many real problems. Hence the concept of multistate system was proposed in [4, 7, 9]. A multistate system has several states $\{0,\dots,M\}$ that range from complete failure to full operation. The components of a multistate system can be binary or multistate. We adress in this work the multistate versions of k-out-of-n systems.

In this paper we denote the components of a system S by $x_1,\dots,x_n$, each of which can be in a set of states $\mathcal{S}_i=\{0,\dots,m_i\}$. The system itself can be in a set of states $\mathcal{S}=\{0,\dots,m\}$. The structure function $\phi:\mathcal{S}_1\times\cdots\times\mathcal{S}_n\to\mathcal{S}$ of S outputs the state of the system in terms of the states of each of the components.

1. k-out-of-n multistate system: definitions

The first definition of multistate k-out-of-n systems is due to El-Neweihi *et. al.* [4].

Definition 1.1 (El-Neweihi *et. al.*, 1978)**.** Let S be a system $\{x_1,\dots,x_n\}$ with n components in which every component can reach a finite number of states $\mathcal{S}=\{0,1,\dots,i\}$. The system S is a *multistate k-out-of-n system* if its structure function $\phi:\mathcal{S}^n\to\mathcal{S}$ satisfies

$$\phi(\mathbf{x})=x_{(n-k+1)},$$

where $\mathbf{x}=(x_1,\dots,x_n)$ denotes the vector of states of components $\{x_1,\dots,x_n\}$ and $x_{(1)}\le x_{(2)}\le\cdots\le x_{(n)}$ is a non decreasing arrangement of $x_1,\dots,x_n$.

Later, Boedigheimer and Kapur [2] defined multistate k-out-of-n on a probabilistic way:

Definition 1.2 (Boedigheimer and Kapur, 1994)**.** ϕ is a multistate k-out-of-$n:G$ structure function if, and only if, ϕ has $\binom{n}{k}$ lower boundary points to level j $(j=1,\dots,M)$ and $\binom{n}{k-1}$ upper boundary points to level j $(j=0,\dots,M-1)$.

A new definition was given in [5] by Huang, Zuo and Wu, which does not require the same number of components to be in a certain state to determine the state of the system. See [5, 6] for the reliability evaluation and numerical examples of these systems.

Definition 1.3 (Huang, Zuo and Wu, 2000)**.** An n-component system is called a *generalized multistate k-out-of-n:G system* if $\phi(\mathbf{x}) > j,\ 1 \leq j \leq M$ whenever there exist and integer value l $(j \leq l \leq M)$ such that at least k_l components are in state l or above.

Zuo and Tian give in [13] a new definition of multistate k-out-of-$n : F$ system:

Definition 1.4 (Zuo and Tian, 2006)**.** An n-component system is called *generalized multistate k-out-of-$n : F$ system* if $\phi(\mathbf{x}) < j,\ 1 \leq j \leq M$ whenever the states of at least k_l components are below l for all l such that $j \leq l \leq M$. If $k_1 \leq k_2 \leq \cdots \leq k_M$, the system is called *increasing multistate k-out-of-$n : G$ system* otherwise it is a *decreasing multistate k-out-of-$n : G$ system.*

In [10] Sáenz-de-Cabezón defines the following systems:

Definition 1.5. Let S be a system with n components in which every component can reach a finite number of states $\{0, 1, \ldots, i\}$. S is an *i-multistate k-out-of-$n : F$ system* if S fails whenever the sum of the states of its components reaches level k.

Along with the different definitions of multistate k-out-of-n systems, several methods to compute their reliability have been proposed. In [13] an efficient recursive method to calculate the reliability of a multistate k-out-of-$n : F$ system based on minimal cut vectors is given. The method in [1] works for an arbitrary multistate k-out-of-$n : G$ system and is fast and works for large systems. Zaho and Cui propose in [12] a method using the finite Markov chain imbedding (FMCI) approach. Chaturvedi et al. propose in [3] an efficient method and a detailed algorithm to compute the exact reliability of multistate k-out-of-$n : G$ system. Their method is based on conditional probabilities. In [8] a new analytic method based on multi-valued decision diagrams is given.

2. Algebraic analysis of multistate k-out-of-n systems

Our contribution in this paper is the application of the algebraic method in [11] to compute the reliability of k-out-of-$n : G$ systems. This is a general method that can be adapted to all the definitions in the previous section. Let S be a coherent system with n components. Let $\mathcal{F}_{S,j}$ be the set of tuples of components' states $\mathbf{x}$ such that $\phi(\mathbf{x}) \geq j$ for some $0 < j \leq m$. The elements of $\mathcal{F}_{S,j}$ are called *j-working states* of S. Let $\overline{\mathcal{F}}_{S,j}$ be the set of minimal j-working states, i.e. states in $\mathcal{F}_{S,j}$ such that degradation of the performance of any component provokes that the overall performance of the system is degraded to $j' < j$. Let $R = \mathbf{k}[x_1, \ldots, x_n]$ be a polynomial ring over a field $\mathbf{k}$. Each tuple of components' states $(s_1, \ldots, s_n) \in \mathcal{S}_1 \times \cdots \times \mathcal{S}_n$ corresponds to the monomial $x_1^{s_1} \cdots x_n^{s_n}$ in R. The *coherence property* of the system is equivalent to saying that the elements of $\mathcal{F}_{S,j}$ correspond to the monomials in an ideal, denoted by $I_{S,j}$ and called the *j-reliability ideal* of S. The unique minimal monomial generating set of $I_{S,j}$ is formed by the monomials corresponding to the elements of $\overline{\mathcal{F}}_{S,j}$ (see [11, §2] for more details). Hence, obtaining the set of minimal cuts of S amounts to compute the minimal generating set of $I_{S,j}$. In order to compute the *j-reliability* of S (i.e. the probability that the system is performing at least at level j) we

can use the numerator of the Hilbert series of $I_{S,j}$, denoted by $H_{I_{S,j}}$. The polynomial $H_{I_{S,j}}$ gives a formula, in terms of $x_1, \ldots, x_n$ that enumerates all the monomials in $I_{S,j}$, i.e. the monomials corresponding to the states in $\mathcal{F}_{S,j}$. Hence, computing the (numerator of) the Hilbert series of $I_{S,j}$ provides a way to compute the j-reliability of S by substituting x_i^a by $p_{i,a}$, the probability that the component i is at least performing at level a, as explored in [11, §2] (for the binary case). We now give the j-reliability ideals of multistate k-out-of-n systems according to the definitions in the previous section.

Proposition 2.1. *The following is the j-reliability ideal of a k-out-of-n multistate system according to Definition 1.1 and Definition 1.2*

$$I_{(k,n),j} = \langle \prod_{x_i \in \sigma, |\sigma|=k} x_i^j \mid \sigma \subseteq \{1, \ldots, n\} \rangle.$$

Proposition 2.2. *The following is the j-reliability ideal of a k-out-of-n multistate system according to Definition 1.3 and Definition 1.4*

$$I_{(k_l,n),j} = \langle \prod_{x_i \in \sigma, |\sigma|=k_l} x_i^j \mid \sigma \subseteq \{1, \ldots, n\} \rangle$$

Proposition 2.3. *The following is the j-reliability ideal of a k-out-of-n multistate system according to Definition 1.5*

$$I^k_{[n,i]} = \langle x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n} \mid i_1 + i_2 + \cdots + i_n = k \text{ and } i_m = i \text{ for one } m \in \{1, 2, \ldots, n\} \rangle$$

3. Examples and computations

Example 3.1. This is example 8 in [5]. Consider a multistate k-out-of-3 system with four states $(0, 1, 2, 3)$ such that $k_3 = 2$, $k_2 = 2$ and $k_1 = 3$. The probabilities of the different components are $p_{1,0} = 0.1$, $p_{1,1} = 0.2$, $p_{1,2} = 0.3$, $p_{1,3} = 0.4$, $p_{2,0} = 0.1$, $p_{2,1} = 0.2$, $p_{2,2} = 0.2$, $p_{2,3} = 0.6$, $p_{3,0} = 0.1$, $p_{3,1} = 0.2$, $p_{3,2} = 0.4$, $p_{3,3} = 0.3$. We use here the algebraic method to compute the probability that the system is respectively in states 0, 1, 2 and 3 and obtain the same exact results than [5].

For the system to be in state 3 there must be at least 2 components in state 3 or above ($k_3 = 2$). Hence $I_{S_3} = \langle x^3y^3, x^3z^3, y^3z^3 \rangle$. The numerator of the Hilbert series is $H_{I_{S_3}} = x^3y^3 + x^3z^3 + y^3z^3 - 2(x^3y^3z^3)$. Then, the probability that the system is in state 3 or above, denoted $R_{S,3}$, is 0.396, which equals the probability that the system is exactly in state 3, denoted $r_{S,3}$. The system is in state 2 or above if at least 2 components are in state 2 or above, hence $I_{S_2} = \langle x^2y^2, x^2z^2, y^2z^2 \rangle$ and $H_{I_{S_2}} = x^2y^2 + x^2z^2 + y^2z^2 - 2(x^2y^2z^2)$. We obtain $R_{S,2} = 0.826$ and $r_{S,2} = R_{S,2} - R_{S,3} = 0.826 - 0.396 = 0.430$.

Since $k_1 = 3$ the system is in state 1 or above if all 3 components are in state 1 or above or if at least 2 components are in state 2 or above or if at least 2 components are in state 3 or above. $I_{S_1} = \langle xyz, x^2y^2, x^2z^2, y^2z^2 \rangle$, $H_{I_{S_1}} = xyz + x^2y^2 + x^2z^2 + y^2z^2 - (xy^2z^2 + x^2yz^2 + x^2y^2z)$ and we obtain $R_{S,1} = 0.89$ and $r_{S,1} = R_{S,1} - R_{S,2} = 0.89 - 0.826 = 0.064$.

Finally $r_{S,0} = R_{S,0} - R_{S,1} = 1 - 0.89 = 0.11$.

Example 3.2. We consider a multistate k-out-of-3 system given by the Definition 1.1. The system and components can be in three states $\{0, 1, 2\}$. If we work with $k = 1$, the structure function of the system is $\phi(\mathbf{x}) = x_{(3)}$. The probabilities of the different components

are the following: $p_{1,0} = 0.1$, $p_{1,1} = 0.4$, $p_{1,2} = 0.5$, $p_{2,0} = 0.1$, $p_{2,1} = 0.7$, $p_{2,2} = 0.2$, $p_{3,0} = 0.2$, $p_{3,1} = 0.6$, $p_{3,2} = 0.2$. We use here the algebraic method to compute the probability that the system is respectively in states 0, 1 and 2. The system is in state 2 if at least one component is in state 2. Then, the corresponding ideal is $I_{S_2} = \langle x_1^2, x_2^2, x_3^2 \rangle$ and $H_{I_{S_2}} = x_1^2 + x_2^2 + x_3^2 - (x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2) + x_1^2x_2^2x_3^2$. From this, we obtain that the probability that the system is in state 2 is $R_{S,2} = 0.68$. The system is in state 1 or above if at least one component is in state 1, so that $I_{S_1} = \langle x_1, x_2, x_3 \rangle$ and $H_{I_{S_2}} = x_1 + x_2 + x_3 - (x_1x_2 + x_1x_3 + x_2x_3) + x_1x_2x_3$. The probability that the system is in state 1 or above is then $R_{S,1} = 0.762$, and the probability that the system is in state 1 is $r_{S,1} = R_{S,1} - R_{S,2} = 0.762 - 0.68 = 0.082$. Finally, $r_{S,0} = R_{S,0} - R_{S,1} = 1 - 0.762 = 0.238$.

References

[1] Amari S. V., Zuo M. J., Dill G. *A fast and robust reliability evaluation algorithm for generalized multi-state k-out-of-n systems.* IEEE Transactions on Reliability, Vol 58, No 1; 2009.

[2] Boedigheimer R. A., Kapur K. C. *Customer-driven reliability models for multistate coherent systems.* IEEE Transactions on Reliability, Vol 43, No 1; 1994.

[3] Chaturvedi S. K., Besha S. H., Amari S. V., Zuo M. J. *Reliability analysis of generalized multi-state k-out-of-n systems.* J Risk Reliability; 2012.

[4] El-Neweihi E., Proschan F., Sethuraman J. *Multi-state coherent system.* J Applied Probability; 1978.

[5] Huang J., Zuo M. J., Wu Y. *Generalized Multi-state k-out-of-n:G systems.* IEEE Transactions on Reliability, Vol 49, No 1; 2000.

[6] Kuo W., Zuo M. J. *Optimal reliability modeling: principles and applications.* New York: John Wiley & Sons; 2003.

[7] Lisnianski A., Levitin G. *Multi-state system reliability: Assesment, Optimization and Applications.* World Scientific Publishing; 2003.

[8] Mo Y., Liudong X., Amari A. V., Bechta J. *Efficient analysis of multi-state k-out-of-n systems.* Elsevier: Reliability Engineering and System Safety; 2014.

[9] Natvig B. *Multistate systems reliability theory with applications.* John Wiley & Sons; 2011.

[10] Sáenz-de-Cabezón E., *Combinatorial Koszul Homology, Computations and Applications.* Phd. Thesis, Universidad de La Rioja; 2007.

[11] Sáenz-de-Cabezón E., Wynn H. P., *Betti numbers and minimal free resolutions for multistate system reliability bounds.* Journal of Symbolic Computation 44; 2009.

[12] Zhao X., Cui L. R. *Reliability evaluation of generalized multi-state k-out-of-n systems based on FMCI approach.* Int J Syst Sci; 2010.

[13] Zuo M J, Tian Z. *Performance evaluation of generalized multi-state k-out-of-n systems.* IEEE Transactions on Reliability, Vol 55, No 2; 2006.

Universidad de La Rioja
E-mail address: papasco@unirioja.es

Universidad de La Rioja
E-mail address: eduardo.saenz-de-cabezon@unirioja.es

London School of Economics, UK
E-mail address: h.wynn@lse.ac.uk

Monografías de la Real Academia de Ciencias. Zaragoza. **43:** 135–138, (2018).
ISSN: 1132-6360

RATIONAL REPARAMETRIZATION OF ODES WITH RADICAL COEFFICIENTS

J. RAFAEL SENDRA, DAVID SEVILLA, AND CARLOS VILLARINO

Abstract. Given an ordinary differential equation $F(x, y(x), y'(x), \ldots, y^{n)}(x)) = 0$, polynomial in $y, y', \ldots, y^{n)}$ and whose coefficients are complex radical expressions in x, we analyze whether there exists a rational change of variable $x = r(z)$ such that the new differential equation $G(z, Y(z), \ldots, Y^{n)}(z)) = 0$ where $Y(z) = y(r(z))$ is algebraic (i.e. its coefficients are rational in z). We describe an algorithm for this purpose, which provides also the inverse transformation, so that the solutions of both ODEs are related. In the particular case $y'(x) = \delta(x)$ with $\delta(x)$ an algebraic radical expression in x, the algorithm outputs a change of variable into a rational integrand.

Introduction

The resolution of certain families of differential equations by algebraic means is currently an active field. In particular the study of algebraic ordinary differential equations (AODEs), that is, ODEs of the form $F(x, y(x), y'(x), \ldots, y^{n)}(x)) = 0$ where F is a polynomial over the field of rational functions in x; see [GW15], [NTV18] and the references therein. In this paper, we advance the topic by expanding the analysis to equations whose coefficients contain radical expressions (see Example 2.7). More precisely, we consider the ODE

$$F(x, y(x), y'(x), \ldots, y^{n)}(x)) = 0 \tag{1}$$

where F is a polynomial over a field $\mathbb{F}_m$ generated by radical expressions in x with coefficients in the complex field $\mathbb{C}$. Examples of interest can be found in [Kam77]. The general goal is to find, if it exists, a change of variable $x = r(z)$ such that the new differential equation

$$G(z, Y(z), \ldots, Y^{n)}(z)) = 0, \text{ where } Y(z) = y(r(z)) \tag{2}$$

is an algebraic ODE, and so algebra-based methods can be applied. For this, we will utilize results in [SSV17] about rational reparametrization of radical varieties: a radical parametrization is built, and if it is reparametrizable rationally, the resulting change of variable also converts (1) into (2). Also, the inverse of the reparametrization is obtained, which translates any solution of (2) into one of (1).

The second author is a member of the research group GADAC. This research is partially supported by the Spanish Ministerio de Economía y Competitividad and the European Regional Development Fund (ERDF), under Project MTM2017-88796-P; and by Junta de Extremadura and FEDER funds (group FQM024).

1. Preliminaries

In this section we recall some of the basic notions and results on radical varieties; for further details see [SSV17]. In addition, it should be noted that, although most of the results there are for arbitrary dimension, we present them here for the case of curves.

A radical (curve) parametrization is, intuitively speaking, a tuple of complex functions in the variable x belonging to a radical extension of the field $\mathbb{C}(x)$. More precisely, we consider a radical tower $\mathbb{F}_0 = \mathbb{C}(x) \subseteq \cdots \subseteq \mathbb{F}_{m-1} \subseteq \mathbb{F}_m$ such that $\mathbb{F}_i = \mathbb{F}_{i-1}(\delta_i) = \mathbb{F}_0(\delta_1, \ldots, \delta_i)$ with $\delta_i^{e_i} = \alpha_i \in \mathbb{F}_{i-1}$, $e_i \in \mathbb{N}$. Then, a radical parametrization is a tuple $\mathcal{P}$ of elements of $\mathbb{F}_m$ whose Jacobian has rank 1; see Example 2.7.

Given a radical parametrization $\mathcal{P}$, we define the *radical curve* associated to it as the Zariski closure of $\mathrm{Im}(\mathcal{P})$ and denote it as $\mathcal{V}_\mathcal{P}$. On the other hand, we define another curve, called *tower curve* and denoted as $\mathcal{V}_\mathbb{T}$, as follows: let $\psi(x) = (x, \delta_1(x), \ldots, \delta_m(x))$ (note that this is another radical parametrization). Then $\mathcal{V}_\mathbb{T}$ is the Zariski closure of $\mathrm{Im}(\psi)$.

Now, since the components of $\mathcal{P}$ are rational functions in the δ's, we have a rational map $\mathcal{R}\colon \mathcal{V}_\mathbb{T} \to \mathcal{V}_\mathcal{P}$.

Remark 1.1. With the above notations and definitions, the following holds (see [SSV17, Th. 4.11]): $\mathrm{genus}(\mathcal{V}_\mathcal{P}) \leq \mathrm{genus}(\mathcal{V}_\mathbb{T})$; furthermore, if $\mathcal{V}_\mathbb{T}$ is rational then $\mathcal{V}_\mathcal{P}$ is rational. Also, if $\mathcal{T}\colon \mathbb{C} \to \mathcal{V}_\mathbb{T}$ is a parametrization of $\mathcal{V}_\mathbb{T}$ then $\mathcal{R} \circ \mathcal{T}$ is a parametrization of $\mathcal{V}_\mathcal{P}$; note that, if $\mathcal{R}$ is birational and $\mathcal{V}_\mathcal{P}$ is rational then $\mathcal{V}_\mathbb{T}$ is rational.

2. Results and algorithm

We start with a technical lemma.

Lemma 2.1. *Let $x = r(z)$ be a change of variable, and let $Y(z) = y(r(z))$. Then*

$$\begin{pmatrix} y(r(z)) \\ y'(r(z)) \\ \vdots \\ y^{n)}(r(z)) \end{pmatrix} = L(z) \begin{pmatrix} Y(z) \\ Y'(z) \\ \vdots \\ Y^{n)}(z) \end{pmatrix}$$

where L is a lower triangular matrix whose entries are rational functions in $\{r'(z), \ldots, r^{n)}(z)\}$ and such that $\det(L)$ is a power of $\frac{1}{r'(z)}$.

Proof. We will prove by induction $r'(z)^k y^{k)}(r(z)) = Y^{k)}(z) + \sum_{j=1}^{k-1} R_j(r', \ldots, r^{k)}) Y^{j)}(z)$, for $k \in \{0, \ldots, n\}$ for some rational functions R_j in k variables. For $k = 0$ the equality is obvious. Let us assume that it holds for $k = \ell$. Taking derivatives in the expression above for $k = \ell$ we have that, for some rational functions Q_j in $\ell + 1$ variables,

$$\ell \cdot r'(z)^{\ell-1} y^{\ell)}(r(z)) + r'(z)^{\ell+1} y^{\ell+1)}(r(z)) = Y^{\ell+1)}(z) + \sum_{j=1}^{\ell} Q_j(r', \ldots, r^{\ell+1)}) Y^{j)}(z).$$

Applying the hypothesis of induction the formula is proven. □

Remark 2.2. Let $\mathcal{I}$ be the class of all non-constant differentiable functions $r(z)$ such that $r'(z) \in \mathbb{C}(z)$. If $r(z) \in \mathcal{I}$, then the matrix L in the previous lemma has entries in $\mathbb{C}(z)$.

Let $\overline{a}(x) \in \mathbb{F}_m^N$ be the tuple of coefficients of F in (1) for some term order.

Theorem 2.3. *The following are equivalent:*

(i) There exists $r(z) \in \mathcal{I}$ such that (2) is algebraic.

(ii) There exists $r(z) \in \mathcal{I}$ such that all the elements of $\overline{a}(r(z))$ are rational.

Furthermore, if one holds for some r, the other one holds for the same r.

Proof. $(ii) \Rightarrow (i)$ follows from the definition of $\mathcal{I}$ and Lemma 2.1. In order to see that $(i) \Rightarrow (ii)$, let $\overline{w} = (w_0, \ldots, w_n)$ be new variables and define

$$H_1(z, \overline{w}) = F(r(z), \overline{w}) \qquad \text{and} \qquad H_2(z, \overline{w}) = F(r(z), L^{-1}(z) \cdot \overline{w}^T).$$

By (i), $H_2 \in \mathbb{C}(z)[\overline{w}]$. Also, by definition $H_1(z, \overline{w}) = H_2(z, L \cdot \overline{w}^T)$. Now, since $r \in \mathcal{I}$, we have that L is a matrix over $\mathbb{C}(z)$. Therefore, $H_1(z, \overline{w}) \in \mathbb{C}(z)[\overline{w}]$. But the coefficients of $H_1(z, \overline{w})$ w.r.t. $\overline{w}$ are precisely the components of $\overline{a}(r(z))$, and hence (ii) holds. □

The following result gives a sufficient condition to obtain an algebraic ODE. For this purpose, consider the radical parametrization $\mathcal{P}(t) = (t, \overline{a}(t))$ and its associated $\mathcal{V}_\mathcal{P}$, $\mathcal{V}_\mathbb{T}$.

Corollary 2.4. *(i) If $s(z) \in \mathcal{I}$ is such that all the elements of the tuple $\overline{\delta}(s(z))$ are rational, then there exists $r(z) \in \mathbb{C}(z) \subset \mathcal{I}$ such that (2) is algebraic.*

(ii) If $\mathcal{Q}(z) = (r(z), \ldots)$ is a rational parametrization of $\mathcal{V}_\mathbb{T}$, then the ODE (2), obtained applying the change $x = r(z)$ to (1) is algebraic.

(iii) Suppose that $\mathcal{Q}(z)$ in (ii) is proper and let h be its inverse. If $Y(z)$ is a solution of (2), then $Y(h(x, \overline{\delta}(x))$ is a solution of (1).

Proof. (i) and (ii): the hypothesis implies that $\mathcal{V}_\mathbb{T}$ is unirational, and since $\mathcal{V}_\mathbb{T}$ is a curve it is rational (see [SWPDa08]). Therefore, by Remark 1.1, $\mathcal{V}_\mathcal{P}$ is rational. Let $(r(z), \ldots)$ be a rational parametrization of $\mathcal{V}_\mathbb{T}$. Then $(r(z), \overline{a}(r(z))$ is a rational parametrization of $\mathcal{V}_\mathcal{P}$ and so the components of $\overline{a}(r(z))$ are rational. Now the result follows from Theorem 2.3.

The proof of (iii) is a simple check. □

All the previous ideas can be algorithmically treated, as we do next. For this purpose, we will use two auxiliary algorithms (see [SWPDa08] for details):

- RatParamAlg decides whether an algebraic curve is rational and, in the affirmative case, computes a proper rational parametrization.
- InvParamAlg computes the inverse of a proper rational curve parametrization.

Algorithm 2.5 (Algebraic Reparametrization Algorithm for ODEs)**.**

Input: An ODE in the form (1).

Output: EITHER a rational function change of variable $x = r(z)$ such that applying it to (1) yields an algebraic ODE, and a rational function h such that if $Y(z)$ is a solution of (2), then $Y(h(x, \overline{\delta}(x))$ is a solution of (1) **OR** "No answer"

1: Collect in the tuple $\overline{a}$ all coefficients of the differential equation (1).
2: Compute $\mathcal{V}_\mathbb{T}$ for $\mathcal{P} = (t, \overline{a})$ (see [SSV17, Remark 4.7]) and apply RatParamAlg to it.
3: **if** $\mathcal{V}_\mathbb{T}$ has a rational parametrization $\mathcal{Q}(z) = (r(z), \ldots)$ **then**
4: Compute the inverse h as InvParamAlg$(\mathcal{Q})(z)$.
5: **return** $x = r(z)$ and h.
6: **else**

7: **if** $\mathcal{R}\colon \mathcal{V}_{\mathbb{T}} \to \mathcal{V}_{\mathcal{P}}$ is birational **then**
8: **return** "No rational reparametrization exists for our purposes"
9: **else**
10: **return** "No answer"

Remark 2.6. If $\mathcal{R}$ is birational and $\mathcal{V}_{\mathbb{T}}$ is not rational, then $\mathcal{V}_{\mathcal{P}}$ cannot be rational. Therefore there exists no $r(z)$. If $\mathcal{V}_{\mathbb{T}}$ is not rational and $\mathcal{R}$ is not birational, it is possible that $\mathcal{V}_{\mathcal{P}}$ can still be reparametrized somehow.

Example 2.7. Consider the radical ODE $\sqrt{x}\,y''(x)+\sqrt{x+1}+x=0$. Let $\overline{a} = (\sqrt{x}, \sqrt{x+1}+x)$ and $\mathcal{P} = (x, \sqrt{x}, \sqrt{x+1}+x)$. Define $\delta_1 = \sqrt{x}$ and $\delta_2 = \sqrt{x+1}$. The tower variety is the closure of the image of $t \mapsto (t, \delta_1(t), \delta_2(t))$. It is an irreducible space curve with equations $\Delta_1^2 - T, \Delta_2^2 - T - 1$. It is rational, with a parametrization $\mathcal{Q}(z) = \left(\frac{z^4-2z^2+1}{4z^2}, \frac{z^2-1}{2z}, \frac{z^2+1}{2z}\right)$. Therefore, substituting $x = \frac{z^4-2z^2+1}{4z^2}$ into the original ODE we obtain

$$\frac{2z^5Y''(z)}{(z-1)(z+1)(z^2+1)^2} - \frac{2z^4(z^4+3)Y'(z)}{(z^2+1)^3(z-1)^2(z+1)^2} + \frac{z^4+2z^3-2z^2+2z+1}{4z^2} = 0$$

that is algebraic as expected. The inverse of $\mathcal{Q}$ is $h(x_1, x_2, x_3) = (x_3 - x_2)^{-1}$ which can be used to recover solutions of the first ODE from those of the latter one, via the change $z = h(x, \delta_1(x), \delta_2(x)) = \sqrt{x+1} + \sqrt{x}$.

References

[GW15] Georg Grasegger and Franz Winkler. Symbolic solutions of first-order algebraic ODEs. In *Computer algebra and polynomials*, volume 8942 of *Lecture Notes in Comput. Sci.*, pages 94–104. Springer, Cham, 2015.

[Kam77] Erich Kamke. *Differentialgleichungen*. B. G. Teubner, Stuttgart, 1977. Lösungsmethoden und Lösungen. I: Gewöhnliche Differentialgleichungen, Neunte Auflage, Mit einem Vorwort von Detlef Kamke.

[NTV18] Franz Winkler N. Thieu Vo, Georg Grasegger. Deciding the existence of rational general solutions for first-order algebraic odes. *J. of Symb. Comp.*, 87:127–139, 2018.

[SSV17] J. Rafael Sendra, David Sevilla, and Carlos Villarino. Algebraic and algorithmic aspects of radical parametrizations. *Comput. Aided Geom. Design*, 55:1–14, 2017.

[SWPDa08] J. Rafael Sendra, Franz Winkler, and Sonia Pérez-Dí az. *Rational algebraic curves*, volume 22 of *Algorithms and Computation in Mathematics*. Springer, Berlin, 2008. A computer algebra approach.

[First and third authors] Research Group ASYNACS. Dpto. de Física y Matemáticas, Universidad de Alcalá, 28871 Alcalá de Henares (Madrid), Spain

E-mail address: rafael.sendra@uah.es, carlos.villarino@uah.es

[Second author] Centro U. de Mérida, Univ. de Extremadura, Av. Santa Teresa de Jornet 38, 06800 Mérida (Badajoz), Spain

E-mail address: sevillad@unex.es