EACA 2014

Barcelona, June 18th–20th, 2014

Edited by
Joan Elias, Jesús Fernández-Sánchez,
and Martin Sombra

Conference
Encuentros de Álgebra Computacional y Aplicaciones
Barcelona, June 2014

I.S.B.N. 978-84-697-0651-0

Encuentros de Álgebra Computacional y Aplicaciones

Barcelona 2014

Edited by
Joan Elias, Jesús Fernández-Sánchez,
and Martin Sombra

Sponsors

Universitat de Barcelona

Universitat Politècnica de Catalunya

IMUB Institut de Matemàtica

Facultat de Matemàtiques i Estadística
Universitat Politècnica de Catalunya

Societat Catalana de Matemàtiques

Real Sociedad Matemática Española

Ministerio de Economía y Competitividad

Contents

Foreword

The EACA's or "Encuentros de Álgebra Computacional y Aplicaciones" (Meetings on Computer Algebra and Applications) are organized by the Spanish "Red Temática de Cálculo Simbólico, Álgebra Computacional y Aplicaciones". They provide a meeting frame for researchers in the fields of Computer Algebra and Symbolic Computation, and for those who use these techniques in their research. We emphasize and specially favor the participation of young researchers.
This XIV Meeting (biannual since 2002) is the natural continuation of those organized in Santander (1995), Sevilla (1996), Granada (1997), Sigüenza (1998), Tenerife (1999), Barcelona (2000), Ezcaray (2001), Valladolid (2002), Santander (2004), Sevilla (2006), Granada (2008), Santiago de Compostela (2010), and Alcalá de Henares (2012). During these years, the conference has achieved a remarkable relevance and prestige within the Symbolic Computation community. The main subjects of interest of the meetings are:

- 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 to Science and Technology

EACA 2014 will take place in Barcelona, at the Institut d'Estudis Catalans from June 18th to 20th, 2014.

This book contains the extended abstracts of the accepted contributions as well as of the plenary talks. EACA2014 has 34 contributions, accepted after a standard referee process, and 5 plenary talks. The plenary speakers are:

- Elisenda Feliu, University of Copenhagem, Denmark
- Deepak Kapur, University of New Mexico, USA
- Manuel Ladra, University of Santiago de Compostela, Spain
- Bernard Mourrain, INRIA Sophia-Antipolis, France
- Francisco Santos, University of Cantabria, Spain

We would like to express our gratitude to the members of the Scientific Committee: María Emilia Alonso (U. Complutense de Madrid), Isabel Bermejo (U. La Laguna), Francisco J. Castro (U. Sevilla), Carlos D'Andrea (U. Barcelona), Joan Elías (U. Barcelona), Philippe Giménez (U. Valladolid), José Gómez-Torrecillas (U. Granada, *Chair*), Laureano González-Vega (U. Cantabria), Manuel Ladra (U. Santiago de Compostela), Antonio Montes (U. Politècnica de Catalunya), Tomás Recio (U. Cantabria), Julio Rubio (U. La Rioja), and J. Rafael Sendra (U. Alcalá de Henares), and of the Local Committee: María Alberich (U. Politècnica de Catalunya), Josep Àlvarez (U. Politècnica de Catalunya), Marta Casanellas (U. Politècnica de Catalunya), Gemma Colomé-Nin (U. Pompeu Fabra), Teresa Cortadellas (U. Barcelona), Carlos D'Andrea (U. Barcelona, *Chair*), Joan Elías (U. Barcelona), Alberto Fernández (U. Pompeu Fabra), Jesús Fernández (U. Politècnica de Catalunya), Antonio Montes (U. Politècnica de Catalunya), Marta Narváez (U. Barcelona), and Martín Sombra (ICREA & U. Barcelona).

The success of EACA2014 is possible because of the efforts of these people.

Finally, we would like to thank to the following institutions for their financial support: Universitat de Barcelona, Institut de Matemàtica de la Universitat de Barcelona, Universitat Politècnica de Catalunya, Facultat de Matemàtiques i Estadística (UPC), Societat Catalana de Matemàtiques, Real Sociedad Española de Matemáticas, Ministerio de Economía y Competitividad.

We wish to all participants a successful conference and a very pleasant stay in the city of Barcelona.

Joan Elías, Jesús Fernández, and Martín Sombra
Barcelona, June 2014

Acknowledgements

Institutions

Universitat de Barcelona
Facultat de Matemàtiques de la UB
Departament d'Àlgebra i Geometria, FM-UB
Institut de Matemàtica de la UB
Universitat Politècnica de Catalunya
Facultat de Matemàtiques i Estadística de la UPC
Departament de Matemàtica Aplicada 1 UPC
Societat Catalana de Matemàtiques
Real Sociedad Matemàtica Española
Ministerio de Economía y Competitividad

Projects

Red Temática de Cálculo Simbólico, Álgebra Computacional y Aplicaciones.
MTM2010-19336: Métodos Efectivos en Álgebra: D-Módulos y Representaciones
MTM2010-20279: Métodos Efectivos en Álgebra Conmutativa y en Geometria Algebraica
MTM2012-38122-C03-02 Geometría algebraica, simpléctica y aritmética
MTM2012-38122-C03-01 Geometría algebraica, simpléctica, aritmética y aplicaciones

and very specially to
Raquel Caparrós (U.P.C.)

Scientific program

Wednesday June 18th

8:30-9:30	Registration
9:15-9:30	Opening ceremony
9:30-10:30	Francisco Santos
	Triangulaciones unimodulares de polítopos reticulares
10:30-11:00	Coffee break
11:00-11:30	Matthew England
	Formulating Problems for Real algebraic Geometry
	Manuel Ceballos
	A note on the representation of solvable Lie Algebras
11:30-12:00	Mohamed S. Boudellioua
	Reduction of Roesser's 2-d linear discrete systems using symbolic computation
	Gabriel Navarro
	A similarity test for Ore polynomials
12:00-12:30	Luis Felipe Tabera
	Ultraquadrics associated to affine and projective automorphisms
	Eulàlia Montoro
	Determinant of any matrix that belongs to $Z(J)$
12:30-13:00	Steven Thorton
	Zigzag form over families of parametric matrices
	Maximilian Jaroschek
	Radicals of Ore polynomials
15:00-16:00	Deepak Kapur
	An algorithm for computing a minimal comprehensive Gröbner basis of a parametric polynomial system
16:00-16:30	Coffee break
16:30-17:00	Eva García-Llorente
	A semigroup approach to projective monomial curves associated to arithmetic sequences
	Gema Díaz-Toca
	The confluent Bezout matrix
17:00-17:30	Aureliano Robles-Pérez
	Families of numerical semigroups: Frobenious pseudo-varieties and trees associated to them
	Maria-Laura Torrente
	Perturbation results on polynomial zero-loci
17:30-18:00	Ignacio García-Marco
	On the Möbius function of semigroups of N
	Mario Fioravanti
	Null Space of the Bezout Matrix and GCD's

Thursday June 19th

9:30-10:30	Elisenda Feliu *How can progress in algebra help systems biology?*
10:30-11:00	Coffee break and group picture
11:00-11:30	Alberto F. Boix *An algorithm for producing F-pure ideals* Ekatherina A. Karatsuba *Algorithms for computation of trascendental functions with near to optimal complexity*
11:30-12:00	Ferran Dachs-Cadefau *Computing jumping numbers and multiplier ideals in two-dimensional regular local rings* Christian Eder *Signature-Based Gröbner bases algorithms in Singular*
12:00-12:30	Eduardo Sáenz-de-Cabezón *Pommaret-Seiler resolution is cellular* Laura Colmenarejo *Some stability phenomena for the reduced Kronecker coefficients*
12:30-13:00	Teresa Cortadellas *The Rees Algebra of a monomial plane parametrization* Robert Moir *Unwinding paths on the Riemann Sphere for continuous integrals of rational functions*
15:00-15:30	Gadea Mata *Zigzag homology for biomedical image processing* Matteo Gallet *Bond theory for pentapods and hexapods*
15:30-16:00	Douglas Navarro Guevara *Representation of functions for an efficient CAS* Rafael Sendra *A critical set of revolution surface parametrizations*
16:00-16:30	Coffee break
16:30-17:00	Carlos D'Andrea *Hilbert's Nullstellensatz and polynomial dynamical systems* Cristina Bertone *The scheme of Liftings and Applications*
17:00-17:30	Fanxuan Zeng *Nonlinear Q-ary codes: Constructions and minimum distance computation* Marta Abril Bucero *New polynomial optimization algorithm using border basis*
20:30	Social dinner: *Ca la Nuri*

Friday June 20th

9:30-10:30	Bernard Mourrain *Sparse modeling and applications*
10:30-11:00	Coffee break
11:00-11:30	André Galligo *On detection of solitary waves, using phase diagrams and real discriminants* Nelly Villamizar *Ring structures of splines on triangulations*
11:30-12:00	Jesús Fernández Sánchez *Complete intersection for phylogenetic group-based model*
12:00-13:00	Manuel Ladra *Gröbner bases and nonassociative algebras. Some applications*
17:00-20:00	Social activity: *Guided Walking tour through architectural modernism in Barcelona*

Plenary talks

HOW CAN PROGRESS IN ALGEBRA HELP SYSTEMS BIOLOGY?

ELISENDA FELIU

ABSTRACT. It is widespread in biology to model the time evolution of species concentrations in reaction networks with systems of ordinary differential equations. When analyzed appropriately, these models can be used to understand and predict the behavior of biological systems. Current models in systems biology employ polynomial dynamical system and as a consequence the steady states of the model are the zeros of a system of polynomial equations. These systems are often parameterised by unknown parameters and, further, only positive solutions have a physical meaning. Therefore, it is of interest to study the positive zeros of a parameterised family of polynomials.

In the talk I will present the framework of the theory of reaction networks and give an overview of questions that are relevant for systems biology. Emphasis will be put on the open questions, to encourage further development of algebraic methods to address the questions of interest.

In the last part of the talk I will present some of my own results. Some of the results involve collaborations with Carsten Conradi, Alicia Dickenstein, Varun Kothamanchu, Stefan Müller, Georg Regensburger, Anne Shiu, Orkun Soyer, and Carsten Wiuf.

INTRODUCTION

Motivation. Systems of ordinary differential equations (ODEs) are traditionally used for quantitative modeling of systems of interacting species. Classical examples include the Lotka-Volterra predator-prey system, proposed independently in the context of chemical reactions and animal interactions [16]; epidemiological models such as the SIR model [1]; and the Hodgkin-Huxley model for the action potential in the squid giant axon [11]. In biochemistry, enzyme kinetics experienced a break-through when Michaelis and Menten employed ODEs to describe the time evolution of the concentration of the product of an enzymatic reaction.

Systems of ODEs, often based on the principle of the law of mass-action or various modifications of it, provide a mechanistic description of complex (chemical) reaction networks. A careful analysis of such systems provides a detailed understanding of the system's possible behaviors and offers the possibility to predict the outcome of the system under changing conditions.

Systems biology aims at understanding how the cell operates as a whole, by taking into consideration all the biochemical reactions occurring at once. An accurate theoretical analysis of the dynamics of the resulting ODE systems is often difficult because of the large number of variables and unknown parameters in the system. Therefore, the area of systems biology will benefit from the development of mathematical techniques to analyze ODE models of reaction networks.

1. ALGEBRA AND REACTION NETWORKS

ODE equations arising from reaction networks have a specific structural form. A *reaction network* consists of a set of reactions between species. For example, a chemical transformation from A to B catalyzed by C can be represented by the reaction $A + C \to B + C$. More generally, a reaction is represented by an arrow between two linear combinations of the elements in some set of *species* $\mathcal{X} = \{X_1, \dots, X_n\}$:

$$r\colon a_1X_1 + \cdots + a_nX_n \to b_1X_1 + \cdots + b_nX_n. \tag{1}$$

The concentration of species X_i is denoted by x_i and the vector of concentrations is $x = (x_1, \dots, x_n)$.

With the hypothesis of *mass-action kinetics*, it is assumed that the reaction occurs at a rate given by

$$K_r(x) = \kappa_r x_1^{a_1} \cdot \ldots \cdot x_n^{a_n},$$

where $\kappa_r > 0$ is a reaction rate constant. Then, the ODE system that models the concentrations of the species is built by simultaneously considering the reaction rates of all reactions:

$$\dot{x}_i = f_{\kappa,i}(x) = \sum_{\text{reactions } r} (\text{net production of species } i \text{ in reaction } r) K_r(x). \tag{2}$$

The reaction rate constants κ_r are *parameters* of the system, and may or may not be known in advance.

For example, if the reaction set is $r_1\colon X_1 + X_2 \to 2X_3$ and $r_2\colon X_1 + X_3 \to X_2$ then the choice of mass-action rates implies that $K_1(x) = \kappa_1 x_1 x_2$ and $K_2(x) = \kappa_2 x_1 x_3$ and the ODE system becomes:

$$\begin{aligned} \dot{x}_1 &= -\kappa_1 x_1 x_2 - \kappa_2 x_1 x_3 \\ \dot{x}_2 &= -\kappa_2 x_1 x_2 + \kappa_2 x_1 x_3 \\ \dot{x}_3 &= 2\kappa_3 x_1 x_2 - \kappa_2 x_1 x_3. \end{aligned}$$

Observe that by definition, the obtained ODE system is polynomial.

By letting $f_\kappa(x) = (f_{\kappa,1}(x), \dots, f_{\kappa,n}(x))$, the steady states of the system are found by solving the system of polynomial equations

$$f_\kappa(x) = 0. \tag{3}$$

Algebraic theory of reaction networks aims to understand the reaction networks near a steady state by taking advantage of the algebraic structure of the steady state equations.

2. Overview of the challenges

As already mentioned, the value of the parameters κ is often unknown. Therefore, it is of interest to study the solutions to equation (3) for all possible values of κ. Furthermore, only positive solutions are relevant in the biological context and hence the object of study are the positive, or maybe nonnegative, solutions to (3).

Recent work has demonstrated how algebraic tools can be employed to determine properties of the steady states that do not depend on the choice of parameters κ, and also to determine if the positive solutions to equation (3) can exhibit some specific property for some choice of the parameters.

For example, a relevant question in systems biology, because it is associated with cell differentiation and on-off responses, is to determine whether equation (3) admits multiple positive solutions for some value of the parameters κ. There exist several methods (e.g. [2, 4–6, 14, 15, 17], to name a few) to determine whether the system will admit a unique positive steady state for all values of κ or whether multiple such solutions exist for some κ. This question can be studied in relation to the injectivity of the map f_κ.

Another relevant question, which can be addressed using elimination theory, is to determine whether there exist elements in the ideal generated by the components of $f_\kappa(x)$ that can be used for model selection, that is, to determine the reaction network underlying some experimental data [9, 10, 13].

Finally, models of the same biochemical system might have very different properties depending on the form of the reactions and the specific details of the models, and therefore the properties of the steady states may depend on the accuracy of the choice of the model. Some progress has been made towards understanding how properties at steady state of a submodel or a reduced model relate to properties of the full model [3, 7, 8, 12], even when the parameters are unknown.

These are some of the questions that have already been addressed, but a complete theory that links a given reaction network to the emergence of one of the properties above is far from complete. For instance, there does not exist a general method that can be applied to an arbitrary network to conclude whether equation (3) can have multiple positive solutions for some choice of parameters. Moreover, there are other pertinent areas that also require investigation. Perhaps the more relevant is the lack of a method to divide the parameter space (i.e. the values of κ) into regions where equation (3) has a different number of solutions.

The talk. In the talk I will start by providing the framework of the theory. I will proceed to give an overview of questions that are relevant for systems biology, with emphasis on the open questions. In the last part of the talk I will present some of my own results.

The results I will present involve collaborations with Carsten Conradi, Alicia Dickenstein, Varun Kothamanchu, Stefan Müller, Georg Regensburger, Anne Shiu, Orkun Soyer, and Carsten Wiuf.

References

[1] B. M. Anderson and R. M. May. *Infectious Diseases of Humans: Dynamics and Control.* Oxford University Press, Oxford, fifth edition, 1991.

[2] M. Banaji and G. Craciun. Graph-theoretic approaches to injectivity and multiple equilibria in systems of interacting elements. *Commun. Math. Sci.*, 7(4):867–900, 2009.

[3] C. Conradi, D. Flockerzi, J. Raisch, and J. Stelling. Subnetwork analysis reveals dynamic features of complex (bio)chemical networks. *Proc. Nat. Acad. Sci.*, 104(49):19175–80, 2007.

[4] G. Craciun and M. Feinberg. Multiple equilibria in complex chemical reaction networks. I. The injectivity property. *SIAM J. Appl. Math.*, 65(5):1526–1546, 2005.

[5] M. Feinberg. Chemical reaction network structure and the stability of complex isothermal reactors I. The deficiency zero and deficiency one theorems. *Chem. Eng. Sci.*, 42(10):2229–68, 1987.

[6] E. Feliu and C. Wiuf. Preclusion of switch behavior in reaction networks with mass-action kinetics. *Appl. Math. Comput.*, 219:1449–1467, 2012.

[7] E. Feliu and C. Wiuf. Simplifying biochemical models with intermediate species. *J. R. S. Interface*, 10:20130484, 2013.

[8] E. Feliu and C. Wiuf. Variable elimination in post-translational modification reaction networks with mass-action kinetics. *J. Math. Biol.*, 66(1):281–310, 2013.

[9] J. Gunawardena. Distributivity and processivity in multisite phosphorylation can be distinguished through steady-state invariants. *Biophys. J.*, 93:3828–3834, 2007.

[10] H. A. Harrington, K. L. Ho, T. Thorne, and M. P. H. Stumpf. Parameter-free model discrimination criterion based on steady-state coplanarity. *Proc. Natl. Acad. Sci.*, 109:15746–15751, 2012.

[11] A. L. Hodgkin and A. F. Huxley. A quantitative description of membrane current and its application to conduction and excitation in nerve. *J. Physiol.*, 117(4):500âĂŞ544, 1952.

[12] B. Joshi and A. Shiu. Atoms of multistationarity in chemical reaction networks. *J. Math. Chem.*, 51(1):153–178, 2013.

[13] A. K. Manrai and J. Gunawardena. The geometry of multisite phosphorylation. *Biophys. J.*, 95:5533–5543, 2008.

[14] S. Müller, E. Feliu, G. Regensburger, C. Conradi, A. Shiu, and A. Dickenstein. Sign conditions for the injectivity of polynomial maps in chemical kinetics and real algebraic geometry. 2014.

[15] S. Müller and G. Regensburger. Generalized mass action systems: Complex balancing equilibria and sign vectors of the stoichiometric and kinetic-order subspaces. *SIAM J. Appl. Math.*, 72:1926–1947, 2012.

[16] J. D. Murray. *Mathematical Biology: I. An introduction*, volume 17 of *Interdisciplinary Applied Mathematics*. Springer, third edition, 2002.

[17] M. Pérez Millán, A. Dickenstein, A. Shiu, and C. Conradi. Chemical reaction systems with toric steady states. *Bull. Math. Biol.*, 74:1027–1065, 2012.

Department of Mathematical Sciences, University of Copenhagen, Universitetsparken 5, 2100 Copenhagen, Denmark

E-mail address: efeliu@math.ku.dk

AN ALGORITHM FOR COMPUTING A MINIMAL COMPREHENSIVE GRÖBNER BASIS OF A PARAMETRIC POLYNOMIAL SYSTEM

DEEPAK KAPUR, YIMING YANG

ABSTRACT. An algorithm to generate a minimal comprehensive Gröbner basis of a parametric polynomial system from an arbitrary faithful comprehensive Gröbner system is presented. The key idea used is that of a polynomial being essential with respect to a comprehensive Gröbner basis.

1. INTRODUCTION

The concepts of a comprehensive Gröbner system (CGS) and a comprehensive Gröbner basis (CGB) were introduced by Weispfenning [14] to associate Gröbner basis like objects for parametric polynomial systems (see also the notion of a related concept of a parametric Gröbner basis independently introduced by Kapur [1]). For a specialization of parameters, a Gröbner basis of the specialized ideal can be immediately recovered from the associated CGS and CGB. This property of CGS and CGB makes them very attractive in applications where a family of related problems can be parameterized and specified using a parametric polynomial system. For various specializations, they can be solved by specializing a parametric solution without having to repeat the computations.

Because of their applications, these topics have been well investigated by researchers and a number of algorithms have been proposed to construct such objects for parametric polynomial systems ([7], [15],[11], [12], [13], [5], [10], [16], [6], [8], [2], [3]). An algorithm by simultaneously generating a comprehensive Gröbner system and a comprehensive Gröbner basis by Kapur, Sun and Wang (KSW) [3] is particularly noteworthy because of its many nice properties: (i) fewer segments (branches) in a comprehensive Gröbner system generated by the algorithm, (ii) all polynomials in a CGS and CGB are faithful meaning that they are in the input ideal, and more importantly, (iii) the algorithm has been found efficient in practice [9].

For the non-parametric case, Gröbner bases have a very nice property: once an admissible term ordering is fixed, every ideal has a canonical Gröbner basis associated with it; a canonical Gröbner basis is not only unique but also reduced and minimal. This property is quite useful in many applications since equality of two ideals can be easily checked by checking the equality of their unique reduced minimal Gröbner bases. The goal of this paper is to work towards a similar property for parametric ideals. The problem addressed is to define a minimal CGB associated with a parametric ideal once an admissible term ordering (both on the parameters as well as variables) is fixed; this seems to be the first step toward defining a canonical CGB.

There are some proposals in the literature for defining a canonical CGB which are not satisfactory. Consider for instance, Weispfenning's proposal in [15]: without reproducing his definition, we give an example of a parametric ideal from his paper generated by a basis $\{f : uy + x, g : vz + x + 1\}$; Weispfenning reported $\{f, g, h, -h\}$ as a canonical CGB of the ideal, where h is $vz - uy + 1$ using the lexicographic ordering $z > y > x > v > u$.

We claim that each of f, g, h is **essential** whereas $-h$ is not: for any specialization σ, if $\sigma(h)$ is in a GB of $\sigma(I)$, then $\sigma(-h)$ is reducible using $\sigma(h)$ and vice versa; so only the *smaller* of the two has to be in a minimal CGB, which is h because though their leading coefficients only differ on the sign,

h is monic while $-h$ is not. Obviously both f and g are essential: for σ in which $uv \neq 0$, $\sigma(f)$ has leading term y while both the other two have z; for σ in which $v = 0$ but $u \neq 0$, $\sigma(g)$ has leading term x while both the other two have y. Further, since $h = g - f$, the GB theory in the nonparametric case might also indicate that h is not essential, but that is not true: for the case $u = 0, v = 0, \sigma(I) = \langle 1 \rangle$, however, $\{\sigma(f) = x, \sigma(g) = x + 1\}$ cannot be a GB of $\sigma(I)$ by itself, whence h is essential. Thus the algorithm proposed in the paper generates $\{f, g, h\}$ as the minimal CGB of this parametric ideal, regardless of the order in which these polynomials are checked for essentiality (see Section 4).

Notice from this example that the minimal CGB is not reduced (since h can be reduced using g), and its specializations are neither reduced nor minimal. There are examples also of minimal CGBs which are reduced but their specializations are neither reduced nor minimal.

Montes and Wibmer [8] also define an object related to a canonical CGS in [8]; but unfortunately, this object cannot be used to generate a canonical CGB since elements in the CGS are not faithful, i.e., not in the original ideal.

We give an algorithm for generating a minimal CGB from a given CGS having the property that associated with every segment describing parameter specialization, there is a GB for that specialization in which every polynomial is in the original ideal, i.e., faithful. For illustration, we use $(I, >)$ as input to this algorithm, the output CGB, which is the union of all GBs associated with each segment in CGS, generated by the KSW algorithm. Recall that every polynomial in CGB generated by the KSW algorithm is faithful since every polynomial in the GB of every segment of its CGS is faithful.

2. Preliminaries

Because of lack of space, we briefly review some key definitions; for a detailed discussion, the reader can refer to [3]. Let $>$ be an admissible total term ordering in which $X \gg U$, variables are bigger than parameters. Below, we need to compare polynomials as elements of $K[U, X]$ as well as elements of $K[U][X]$ using $>$.

A finite subset CG of a parametric ideal $I \subseteq K[U, X]$ is called a *comprehensive Gröbner basis* of I w.r.t. $>$ if and only if for every specialization σ of parameters U in some field L, $\sigma(CG)$ is a Gröbner basis of $\sigma(I)$ w.r.t. the restriction of $>$ considered on terms in X.

It is not required that a CGB be defined for every possible specialization of parameters. Instead, it can be restricted to be defined on a quasi-variety (i.e., branch).

A comprehensive Gröbner basis (CGB) CG of I w.r.t. $>$ is called *minimal* if and only if (i) no proper subset of CG is a CGB of I w.r.t. $>$, and (ii) the leading coefficient of every polynomial in CG when viewed as a polynomial in $K[U, X]$ is monic (which is the same as requiring that the leading coefficient of the polynomial when viewed as a polynomial in variables X is a monic polynomial in parameters U). These conditions are needed since we wish to use a minimal CGB to define a canonical CGB.

A finite set of tuples $\{(A_1, G_1), \ldots, (A_n, G_n)\}$ is a comprehensive Gröbner system (CGS) of I w.r.t. $>$ if and only if and for every σ satisfying A_i, $\sigma(G_i)$ is a Gröbner basis of $\sigma(I)$, where each A_i, called a *segment* (or *branch*), is of the form (E_i, N_i), $A_i = V(E_i) - V(N_i)$ (also written as $V(E_i) \backslash V(N_i)$), and $\bigcup_i A_i$ are all possible specializations of U; σ is said to satisfy A_i if and only if $\sigma \in A_i$, E_i is a finite set of polynomials from $K[U]$, N_i is a finite set of polynomials from $K[U]$.

A reader should notice that in the above definition of a CGS, it is not required that G_i be a subset of I; in fact, there are algorithms for computing a CGS of an I in which G_i need not be a subset. A CGS is called *faithful* if and only each $G_i \subseteq I$. Also notice that the above definition of a CGB requires it to be faithful. The following proposition holds for any CGS generated by the KSW algorithm:

Proposition 2.1. *If a CGS of an ideal $I \subseteq K[U,X]$ w.r.t. an admissible term order $>$ is faithful, for every branch $(A_i, G_i) \in CGS$, G_i is a CGB of I w.r.t. $>$ on A_i.*

3. A polynomial Essential for a Comprehensive Gröbner basis

The key concept used in our algorithm for the generation of a minimal CGB CG of an ideal I is that of a polynomial in CG being essential for a CGB.

A polynomial p is called *essential* w.r.t. a given CGB CG of I if and only if there is a specialization σ such that for any polynomial $q \in CG - \{p\}$, $LT(\sigma(q))$ cannot divide $LT(\sigma(p))$.

Theorem 3.1. *For a given CGB CG of I, (i) if p is not essential w.r.t. CG, then $CG - \{p\}$ is also a CGB of I; (ii) if $p \in CG$ is essential w.r.t. CG, then p remains essential w.r.t. any CGB of I that is a subset of CG.*

Consider the example in Section 1. It is easy to see that only one of h and $-h$ can be essential since for every specialization σ, if $\sigma(h)$ is in a GB of $\sigma(I)$, then $\sigma(-h) = -\sigma(h)$ need not be in the GB.

A polynomial p is said to be *covered* by a finite set $Q = \{q_1, \ldots, q_n\}$ of polynomials over a set A of specializations on parameters iff for every $\sigma \in A$, there is some $q_i \in Q$ such that $LT(\sigma(q_i))$ divides $LT(\sigma(p))$ (thus, $\sigma(q_i)$ is used for reduction whenever $\sigma(p)$ needs to be used). The essentiality of p w.r.t. CG is checked by determining whether it can be covered by polynomials in $CG - \{p\}$ over a subset of parameter specializations for which p is needed. We can optimize this check by having access to the CGS from which a CGB CG of I is computed. In this paper, we assume CGS is the minimal one computed by KSW algorithm. Let $B_p = \{(A_j, G_j)\}_{j \in J}$ be a family of branches in CGS with $p \in G_j$ for each $j \in J$. Then it's enough to consider branches in B_p, since p is guaranteed to be covered over all the others.

In each branch $(A_i, G_i) \in B_p$, let G_{can} be the subset of $CG - G_i$ such that each $g \in G_{can}$ contains some term in X dividing the leading term of p in X. If there is some $g \in G_{can}$ such that $\forall \sigma \in A_i$, $LT(\sigma(g)) \mid LT(\sigma(p))$, then p is covered over this branch and replaced by $g \in G_i$. Otherwise, if $LT(\sigma(g)) \mid LT(\sigma(p))$ for $\sigma \in A_{ic} \subsetneqq A_i$, then A_i is partitioned into A_{ic} and A_{in}, and then specializations in A_{in} needs to be considered for covering of p using $G'_{cand} = G_{cand} - \{g\}$. The checking on A_i continues until either we find some $A_{ess} \subseteq A_i$ such that $LT(\sigma(p))$ is not divisible by $LT(\sigma(G_{can}))$, whence p is essential and the procedure terminates; or we achieve a partition of A_i (possibly just $\{A_i\}$) such that $LT(\sigma(p))$ is divisible by $LT(\sigma(G_{can}))$ for $\forall \sigma \in A_i$, with possibly different polynomials in G_{can} w.r.t. the respective subsets of A_i; afterward, we continue to the next branch in B_p.

If p is covered for every branch in B_p, the procedure terminates declaring p as non-essential.

Lemma 3.2. *Given a polynomial p in a CGB CG of I, p is not essential w.r.t. CG if and only if for every branch (A_i, G_i) in the associated CGS of I such that $p \in G_i$, and for every specialization $\sigma \in A_i$, $LT(\sigma(p))$ is divided by $LT(\sigma(q))$ for some $q \in CG \backslash \{p\}$.*

4. Algorithm for Generating a minimal Comprehensive Gröbner basis

Using the results from the previous section, we informally discuss below an algorithm for computing a minimal CGB due to lack of space; for a more detailed and formal account, as well as proofs, the reader can refer to [4].

Given an ideal $I \subseteq K[U, X]$ and a term ordering $>$, we first compute a comprehensive Gröbner system CGS and a comprehensive Gröbner basis CG of I w.r.t. $>$ using the KSW algorithm. Polynomials in each branch of CGS as well as every polynomial in CG are assumed to require that their leading coefficient is a monic polynomial over the given parameter ring.

Every polynomial p in CG is checked for being essential w.r.t. CG using the procedure described in Section 3, starting with the maximal polynomial in CG w.r.t. $>$ and iterating in descending order. There are two outcomes:

(1) p is not essential: p is not in a minimal CGB generated from CG and can be removed from CG. Further, for checking the essentiality of other polynomials in the updated CG, CGS is updated by replacing each occurrence of p in G_i by the polynomial(s) in $CG - G_i$ covering p for A_i. In particular, if there are multiple polynomials covering p for A_i, then this branch is split into a set of new branches: $\{(A_{ij}, G_{ij})\}_{j \in J}$, in which each G_{ij} is got from G_i by replacing p by the polynomial making p covered for the specializations in A_{ij}, respectively. The algorithm also substitutes these new branches for (A_i, G_i) to update CGS.

(2) p is essential: In this case, p is retained and will be part of a minimal CGB generated from CG. CGS does not change.

In every iteration in which p is checked for being essential, the following invariant holds:

(1) CGS is a CGS of I w.r.t. $>$,

(2) the leading coefficient of every polynomial in CGS when viewed as an element in $K[U, X]$ is monic, and

(3) CG is the union of polynomials in G_i's from CGS and is a CGB of I w.r.t. $>$.

It is easy to see that the algorithm terminates. Upon termination, CG is guaranteed to be an MCGB since it only contains essential polynomials w.r.t. CG.

To illustrate the algorithm, given $F = \{vx + (u - v)y + (u + v)z, (-u + v)x + (u + v)y - vz\} \subseteq K[u, v][x, y, z]$ and a lexicographic order with $x > y > z > u > v$, by the KSW algorithm, we get $CGS = \{(A_1 = (\emptyset, \{(u^2 - uv + 2v^2)v\}), G_1 = \{f_1, f_2\}), (A_2 = (\{u^2 - uv + 2v^2\}, \{v\}), G_2 = \{f_2, f_3\}), (A_3 = (\{u, v\}, \{1\}), G_3 = \emptyset), (A_4 = (\{v\}, \{u^3\}), G_4 = \{f_2, f_4\})\}$ and $CG = \{f_1, f_2, f_3, f_4\}$, where $f_1 = (u^2 - uv + 2v^2)y + (u^2 - 2v^2)z$, $f_2 = vx + (u - v)y + (u + v)z$, $f_3 = (u^2 - uv + 2v^2)x + (-4u^2 + 4uv - 8v^2)y + (-3u^2 + 3uv + 8v^2)z$, $f_4 = ux - 2vy + (u + 2v)z$.

The checking order w.r.t. $>$ is $f_3 > f_4 > f_2 > f_1$. For f_3, it's covered by f_1 in A_2, the only branch in which f_3 appears, thus f_3 is not essential. $CG := CG - \{f_3\}$ and we replace f_3 by f_1 in G_2. Then f_4 is essential due to A_4, f_2 is essential due to a subset of A_1, which is $(\{u\}, \{v(u^2 - uv + 2v^2)\})$, and f_1 is essential due to a subset of A_1, which is $(\emptyset, \{uv(u^2 - uv + 2v^2)\})$.

As a result, $M = \{f_1, f_2, f_4\}$ is a minimal CGB of $\langle F \rangle$ w.r.t. $>$. If polynomials in the CGB generated by the KSW algorithm are checked for essentialness in random order, then there can be three minimal CGBs generated: M, $M' = \{f_1, f_3, f_4\}$, $M'' = \{f_1, f_2, f_3\}$, with $\mathcal{M}$ being minimal among them by extending the polynomial ordering on sets of polynomials.

5. Towards a Canonical Comprehensive Gröbner basis

Since our ultimate goal is to define the concept of a canonical comprehensive Gröbner basis associated with a parametric ideal I, we list below some desired properties of such a CGB:

(1) *Uniqueness:* Given an admissible total term ordering, it should be unique for a given parametric ideal I.

(2) *Faithfulness:* Every polynomial in it should be in I.

The uniqueness property implies that a canonical CGB should be minimal, as otherwise, from a nonminimal canonical CGB, it is possible to identify its proper subset which is also canonical thus contradicting the uniqueness property. The uniqueness property also implies that it should be reduced since otherwise, a polynomial that can be reduced, can be replaced by its reduced form, violating the uniqueness property.

Acknowledgment: The first author would like to thank Prof. Yao Sun for many helpful discussions on this topic. The help provided by Prof. Montes through emails is appreciated.

This research project is partially supported by an NSF award DMS-1217054. Some of this work was done during the first author's sabbatical at the Institute of Software, the Chinese Academy of Sciences in Beijing, China.

REFERENCES

[1] D. Kapur, *An approach for solving systems of parametric polynomial equations*, In: Saraswat, Vijay, Van Hentenryck, Pascal (Eds.), Principles and Practices of Constraints Programming, MIT Press, pp. 217-224, 1995

[2] D. Kapur, Y. Sun, D. Wang, *A new algorithm for computing comprehensive Gröbner systems*, In Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation (pp. 29-36), ACM, 2010

[3] D. Kapur, Y. Sun, D. Wang, *An efficient method for computing comprehensive Gröbner bases*, Journal of Symbolic Computation 52: 124-142, 2012

[4] D. Kapur and Y. Yang, *Algorithms for computing minimal and canonical comprehensive Gröbner bases of parametric polynomial systems.* Forthcoming technical report, Dept. of Computer Science, Univ. of New Mexico, Albuquerque, NM, USA, June 2014.

[5] M. Manubens, A. Montes, *Improving the DISPGB algorithm using the discriminant ideal*, Journal of Symbolic Computation 41.11: 1245-1263, 2006

[6] M. Manubens, A. Montes, *Minimal canonical comprehensive Gröbner systems*, Journal of Symbolic Computation 44.5: 463-478, 2009

[7] A. Montes, *A new algorithm for discussing Gröbner bases with parameters*, Journal of Symbolic Computation 33.2: 183-208, 2002

[8] A. Montes, M. Wibmer, *Gröbner bases for polynomial systems with parameters*, Journal of Symbolic Computation 45.12: 1391-1425, 2010

[9] A. Montes, *Using Kapur-Sun-Wang algorithm for the Gröbner cover*, In Proceedings of EACA 2012. Ed.: J.R. Sendra, C. Villarino. Universidad de Alcalá de Henares., pp. 135-138, 2012

[10] K. Nabeshima, *A speed-up of the algorithm for computing comprehensive Gröbner systems*, Proceedings of the 2007 international symposium on Symbolic and Algebraic Computation (pp. 299-306), ACM, 2007

[11] A. Suzuki, Y. Sato, *An alternative approach to comprehensive Gröbner bases*, Journal of Symbolic Computation 36.3: 649-667, 2003

[12] A. Suzuki, Y. Sato, *Comprehensive Gröbner bases via ACGB*, ACA2004: 65-73, 2004

[13] A. Suzuki, Y. Sato, *A simple algorithm to compute comprehensive Gröbner bases using Gröbner bases*, Proceedings of the 2006 international symposium on Symbolic and Algebraic Computation (pp. 326-331), ACM, 2006

[14] V. Weispfenning, *Comprehensive Gröbner bases*, Journal of Symbolic Computation 14.1: 1-29, 1992

[15] V. Weispfenning, *Canonical comprehensive Gröbner bases*, Journal of Symbolic Computation 36.3: 669-683, 2003

[16] M. Wibmer, *Gröbner bases for families of affine or projective schemes*, Journal of Symbolic Computation 42.8: 803-834, 2007

Dept. of Computer Science, University of New Mexico, Albuquerque, NM, USA
E-mail address: kapur@cs.unm.edu, yiming@cs.unm.edu

GRÖBNER BASES AND NONASSOCIATIVE ALGEBRAS. SOME APPLICATIONS

MANUEL LADRA

ABSTRACT. We will give some applications of Gröbner bases in some specific nonassociative algebras. Specifically, we provide proofs of Poincaré-Birkhoff-Witt theorem for universal enveloping algebras of finite-dimensional Leibniz n-algebras using Gröbner bases in a free associative algebra or we classify these algebras in low dimensions.

In 1965, Buchberger [2] introduced the notion of Gröbner bases for commutative polynomial ideals and an algorithm for their computation. The Gröbner bases provide algorithmic methods to some of the most basic problems in algebraic geometry but are applied also in such diverse areas as cryptography, automated theorem proving in geometry, coding theory, graph theory, statistics, optimization, etc. The theory of Gröbner bases in multivariate polynomial rings over a field is very well known.

Beforehand, in 1962, Shirshov [6] suggested essentially the same ideas for Lie polynomials in Lie algebras.

In 1978, Bergman [1] developed the theory of Gröbner bases for associative algebras by proving the diamond lemma. His idea is a generalization of Buchberger's theory and it has many applications. For noncommutative algebras, Gröbner bases are not guaranteed to be finite.

We recall some of definitions of Gröbner bases in commutative and non-commutative associative algebras summarizing computational differences and similarities when computing Gröbner bases in polynomial rings and non-commutative associative algebras.

In fact, they developed a universal way of computing a basis of an arbitrary algebra of a certain variety. Everything reduces to the properties of relations in the algebra. Shirshov introduced the notion of a composition of Lie polynomials and the notion of a set of polynomials closed under composition. Later on, the sets closed under composition were called the Gröbner bases in the commutative case and considering that Shirshov's method works for associative algebras, Shirshov's theory for Lie algebras and their universal enveloping algebras is called as well the Gröbner-Shirshov basis theory.

Later, we remember some definitions of specific non-associative algebras (Lie algebras, Leibniz algebras, Leibniz n-algebras) and we will apply the Gröbner basis theory to prove Poincaré-Birkhoff-Witt in their universal enveloping algebras or classify them in low dimensions (see [3, 4, 5]).

REFERENCES

[1] G.M. Bergman, *The diamond lemma for ring theory*, Adv. in Math. 29 (1978), 178–218.

[2] B. Buchberger, *An algorithm for finding a basis for the residue class ring of a zero-dimensional polynomial ideal*, Ph. D Thesis, Univ. Innsbruck, Austria, 1965.

[3] J.M. Casas, M.A. Insua, M. Ladra, *Poincaré-Birkhoff-Witt theorem for Leibniz n-algebras*, J. Symbolic Comput. 42 (2007), 1052–1065.

[4] J.M. Casas, M.A. Insua, M. Ladra, S. Ladra, *An algorithm for the classification of 3-dimensional complex Leibniz algebras*, Linear Algebra Appl. 436 (2012), 3747–3756.

[5] M.A. Insua, M. Ladra, *Gröbner bases in universal enveloping algebras of Leibniz algebras*, J. Symbolic Comput. 44 (2009), 517–526.

[6] A.I. Shirshov, *Some algorithm problems for Lie algebras*, Sibirsk. Mat. Zh. 3 (1962), 292–296.

Universidad de Santiago de Compostela
E-mail address: manuel.ladra@usc.es

SPARSE MODELING AND APPLICATIONS

BERNARD MOURRAIN

ABSTRACT. Recovering the structure of a phenomena, a signal or a shape from a set of measurements or observations is a problem which appears in many contexts. We consider here the reconstruction problem of exponential polynomials from truncated moment sequences. Gaspard-Clair-François-Marie Riche de Prony proposed in 1795 a method to solve this problem for functions of one variable. We describe a generalization in several variables. An ingredient of the approach is a flat extension property, which is related to the commutation property of multiplication operators. This is closely connected to border basis computation. We exploit these techniques in a new algorithm to compute the decomposition of series as sums of exponentials. The method is illustrated on several applications, including sparse interpolation, vanishing ideal of points, tensor decomposition.

1. INTRODUCTION

In many context of applications, it is nowadays possible to recover a huge amount of information on a phenomenon that we want to analyse. Sensors, scanners, etc. can produce a deluge of data, which in principle should be helpful to identify the corresponding physical problem or the underlying geometry. But to reduce the complexity of treatment of this huge data set, one usually aims at modeling it by functions which are simpler to manipulate. Recovering this underlying structure boils down to determine a good functional space, in which the function has a sparse representation with few non-zero coefficients and to compute effectively such a representation. This problem known as sparse modeling has an important applications in many domains such as Signal Processing, Image Analysis, Computer Vision, Statistics ...

Hereafter, we concentrate on the following special reconstruction problem:

Problem (Reconstruction from truncated moment sequences): *Given the first coefficients $\sigma_\alpha \in \mathbb{C}$ (up to a degree d) of the series $\sigma(\mathbf{z}) = \sum_{\alpha\in\mathbb{N}^n} \sigma_\alpha \frac{1}{\alpha!}\mathbf{z}^\alpha$, recover the decomposition:*

$$\sum_{i=1}^{r} \omega_i(\mathbf{z}) e^{\xi_{i,1}z_1+\cdots+\xi_{i,n}z_n},$$

that is, the number r of terms, the points $\xi_1,\ldots,\xi_r \in \mathbb{C}^n$ and the polynomial coefficients $\omega_i(\mathbf{z}) \in \mathbb{C}[\mathbf{z}]$. Hereafter, $\mathbf{e}_\xi(\mathbf{z}) = e^{\xi_1 z_1+\cdots+\xi_n z_n}$ for $\xi = (\xi_1,\ldots,\xi_n) \in \mathbb{C}^n$.

Many works have been developed in the one dimensional case ($n = 1$), which refers to the well-known problem of *parameter estimation for exponential sums*. The first contribution on this problem is probably due to Gaspard-Clair-François-Marie Riche de Prony in 1795 [4], who proposed to construct a recurrence relation of minimal size and then to find the roots of the associated characteristic polynomial.

2. Multivariate truncated moment problem

We describe here a generalization of Prony's method in several variables and its main ingredients. Hereafter, $\mathbb{K}$ i a field of characteristic 0 and $\overline{\mathbb{K}}$ its algebraic closure.

2.1. **Duality.**

The dual space $R^* = \mathrm{Hom}_{\mathbb{K}}(\mathbb{K}[\mathbf{x}], \mathbb{K})$ of the ring of polynomials $R = \mathbb{K}[\mathbf{x}]$ is the natural isomorph to the ring of formal power series $\mathbb{K}[[z_1, \ldots, z_n]] = \mathbb{K}[[\mathbf{z}]]$. Namely, if $\Lambda \in R^*$ is an element of the dual of R, it can be represented by the series:

$$\Lambda(\mathbf{z}) \quad = \quad \sum_{\alpha \in \mathbb{N}^n} \Lambda(\mathbf{x}^\alpha) \frac{\mathbf{z}^\alpha}{\alpha!} \in \mathbb{K}[[\mathbf{z}]],$$

This duality is given by the following pairing:

$$\begin{array}{rcl} \mathbb{K}[[\mathbf{z}]] \times \mathbb{K}[\mathbf{x}] & \to & \mathbb{K} \\ (\mathbf{z}^\alpha, \mathbf{x}^\beta) & \mapsto & \langle \mathbf{z}^\alpha | \mathbf{x}^\beta \rangle = \left\{ \begin{array}{ll} \alpha! & \text{if } \alpha = \beta \\ 0 & \text{otherwise}. \end{array} \right. \end{array}$$

so that we have $\langle \Lambda(\mathbf{z}) | \mathbf{x}^\alpha \rangle = \Lambda(\mathbf{x}^\alpha)$.

By construction, the dual space $\mathrm{Hom}_{\mathbb{K}}(\mathbb{K}[\mathbf{x}], \mathbb{K}) \equiv \mathbb{K}[[\mathbf{z}]]$ has a natural structure of $\mathbb{K}[\mathbf{x}]$-module, defined as follows: $\forall \sigma(\mathbf{z}) \in \mathbb{K}[[\mathbf{z}]], \forall p(\mathbf{x}), q(\mathbf{x}) \in \mathbb{K}[\mathbf{x}]$,

$$\langle p(\mathbf{x}) \star \sigma(\mathbf{z}) | q(\mathbf{x}) \rangle \quad = \quad \langle \sigma(\mathbf{z}) | p(\mathbf{x}) q(\mathbf{x}) \rangle.$$

2.2. **Hankel operators.**

Definition 2.1. The Hankel operator associated to an element $\sigma(\mathbf{z}) \in \mathbb{K}[[\mathbf{z}]]$ is

$$\begin{array}{rcl} H_\sigma : \mathbb{K}[\mathbf{x}] & \to & \mathbb{K}[[\mathbf{z}]] \\ p(\mathbf{x}) & \mapsto & p(\mathbf{x}) \star \sigma(\mathbf{z}). \end{array}$$

The kernel $I_\sigma = \{p \in \mathbb{K}[\mathbf{x}] | p \star \sigma = 0\}$ of H_σ is an ideal of $\mathbb{K}[\mathbf{x}]$. Let $\mathcal{A}_\sigma = \mathbb{K}[\mathbf{x}]/I_\sigma$ be the associated quotient algebra.

Definition 2.2. For any $\sigma(\mathbf{z}) \in \mathbb{K}[[\mathbf{z}]]$, the inner product associated to $\sigma(\mathbf{z})$ on $\mathbb{K}[\mathbf{x}]$ is

$$\begin{array}{rcl} \mathbb{K}[\mathbf{x}] \times \mathbb{K}[\mathbf{x}] & \to & \mathbb{K} \\ (p(\mathbf{x}), q(\mathbf{x})) & \mapsto & \langle p(\mathbf{x}), q(\mathbf{x}) \rangle_\sigma := \langle \sigma(\mathbf{z}) | p(\mathbf{x}) q(\mathbf{x}) \rangle \end{array}$$

Since $\forall p(\mathbf{x}), q(\mathbf{x}) \in \mathbb{K}[\mathbf{x}]$, $\langle p(\mathbf{x}) + I_\sigma, q(\mathbf{x}) + I_\sigma \rangle_\sigma = \langle p(\mathbf{x}), q(\mathbf{x}) \rangle_\sigma$, $\langle ., . \rangle_\sigma$ induces an inner product on $\mathcal{A}_\sigma$.

We use the following properties [5]. If $\sigma(\mathbf{z}) = \sum_{i=1}^r \omega_i(\mathbf{z}) \mathbf{e}_{\xi_i}(\mathbf{z})$ with $\omega_i(\mathbf{z}) \in \mathbb{K}[\mathbf{z}] \setminus \{0\}$, then

- the inner product $\langle ., . \rangle_\sigma$ is non-generate on $\mathcal{A}_\sigma = \mathbb{K}[\mathbf{x}]/I_\sigma$.
- the rank of H_σ is $\sum_{i=1}^r \mu_i$ where μ_i is the dimension of the vector space spanned by $\omega_i(\mathbf{z})$ and all its derivatives $\partial_{z_1}^{\alpha_1} \cdots \partial_{z_n}^{\alpha_n} \omega_i(\mathbf{z})$ for $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$;
- the variety $\mathcal{V}_{\overline{\mathbb{K}}}(I_\sigma)$ is the set of points $\xi_1, \xi_2, \ldots, \xi_r \in \mathbb{K}^n$, with multiplicity $\mu_1, \ldots, \mu_r$.

2.3. **The support of** σ**.** We consider now the problem of computing the support $\mathcal{V}_{\overline{\mathbb{K}}}(I_\sigma) = \{\xi_1, \ldots, \xi_r\}$ of a series $\sigma = \sum_{i=1}^{r} \omega_i\,(\mathbf{z})\mathbf{e}_{\xi_i}(\mathbf{z})$ from its Hankel operator H_σ.

We use classical results on the resolution of polynomial equations by eigenvalue and eigenvector of the operators of multiplication $\mathcal{M}_g$ by g in the quotient algebra $\mathcal{A}$ and their transposed :

Proposition 2.3. *Let I be an ideal of $R = \mathbb{K}[\mathbf{x}]$ and suppose that $\mathcal{V}_{\overline{\mathbb{K}}}(I) = \{\xi_1, \xi_2, \ldots, \xi_r\}$. Then*

- *for all $g \in \mathcal{A}$, the eigenvalues of M_g and M_g^t are the evaluations at the polynomial g, namely $g(\xi_1), \ldots, g(\xi_r)$,*
- *The eigenvectors common to all M_g^t with $g \in \mathcal{A}$ are - up to a scalar - the evaluations $\mathbf{e}_{\xi_1}, \ldots, \mathbf{e}_{\xi_r}$.*

Hereafter, $\mathcal{A} = \mathbb{K}[\mathbf{x}]/I$ is the quotient algebra of $\mathbb{K}[\mathbf{x}]$ by any ideal I and $\mathcal{A}^* = \mathrm{Hom}_{\mathbb{K}}(\mathcal{A}, \mathbb{K})$ is the dual of $\mathcal{A}$. It is naturally identified with the orthogonal $I^\perp = \{\Lambda \in \mathbb{K}[[\mathbf{z}]] \mid \forall p \in I, \langle \Lambda, p\rangle = 0\}$.

For our decomposition problem for which $I = I_\sigma$ and $\mathcal{A} = \mathcal{A}_\sigma = \mathbb{K}[\mathbf{x}]/I_\sigma$, we use the following property: For any $g \in \mathbb{K}[\mathbf{x}]$, we have

$$H_{g\star\sigma} = M_g^t \circ H_\sigma = H_\sigma \circ M_g. \tag{1}$$

This allows us to recover the points $\mathcal{V}_{\overline{\mathbb{K}}}(I_\sigma) = \{\xi_1, \xi_2, \ldots, \xi_r\}$ which appears in the exponential part of σ, by eigenvector or eigenvalue computation.

2.4. **Flat extensions.** To solve the truncated moment problem, we use a characterization of all possible extension of the truncated series that have finite rank.

For $\sigma \in \mathbb{K}[[\mathbf{z}]]$ and two subsets B, B' of $\mathcal{M}$, we denote by $H_\sigma^{B,B'}$ the following map:

$$\begin{array}{rcl} H_\sigma^{B,B'} : \langle B\rangle & \rightarrow & \langle B'\rangle^* \\ p(\mathbf{x}) & \mapsto & p(\mathbf{x}) \star \sigma(\mathbf{z})_{|\langle B'\rangle}. \end{array}$$

Definition 2.4. For any matrix H which is a submatrix of another matrix H', we say that H' is a *flat extension* of H if $\operatorname{rank} H = \operatorname{rank} H'$.

To find the decomposition of σ, we use the following result [7]:

Theorem 2.5. *Let B, C be subsets of of $\mathcal{M}$ connected to 1 such that $B^+ \subset C$, $\operatorname{rank} H_\sigma^B = \operatorname{rank} H_\sigma^C = |B|$. Then B is a basis of $\mathcal{A}_\sigma$ and $I_\sigma = (\ker H_\sigma^{B^+})$.*

2.5. **Computing the decomposition.** The algorithm to construct the decomposition of $\sigma(\mathbf{z}) = \sum_{i=1}^{r} \omega_i(\mathbf{z})\mathbf{e}_{\xi_i}(\mathbf{z})$ proceeds as follows:

- Compute incrementally orthogonal polynomials for the inner product $\langle ., .\rangle_\sigma$, until the flat extension criteria is satisfied.
- Deduce a basis B of $\mathcal{A}_\sigma$, a border basis of I_σ with respect to B and the operators of multiplication M_{x_i} $(i = 1, \ldots, n)$ in this basis.
- Compute the common eigenvectors of the transposed operators $M_{x_i}^t$ and deduce the roots $\mathcal{V}_{\overline{\mathbb{K}}}(I_\sigma) = \{\xi_1, \xi_2, \ldots, \xi_r\}$.
- Deduce the weights $\omega_i(\mathbf{z})$ by solving a linear system.

3. Applications

3.1. **Sparse interpolation.** The problem of sparse polynomial interpolation consists in recovering the monomials in the support of the polynomial and their non-zero coefficients, from the evaluation of the polynomial at some points:

$$p(x_1, \dots, x_n) = \sum_{a \in A} w_a \mathbf{x}^a \tag{2}$$

with the support $A \subset \mathbb{Z}^n$ of size r and $\omega_a \in \mathbb{K} \setminus \{0\}$. We want to recover the number r of terms, the support A and the coefficients ω_a.

By transforming the sparse polynomial p into an exponential polynomial and by applying the method described in Section 2, we recover the sparse decomposition.

3.2. **Vanishing ideal of points.** We consider here the problem of computing the vanishing ideal of a given set of points $\xi_1, \dots, \xi_r \in \mathbb{K}^n$, that is, the ideal of polynomials that vanish at these points. By taking $\sigma(\mathbf{z}) = \sum_{i=1}^{r} \mathbf{e}_{\xi_i}(\mathbf{z}) = \sum_{\alpha \in \mathbb{N}^n} \frac{1}{\alpha!} \sigma_\alpha \mathbf{z}^\alpha$. Its coefficients are $\sigma_\alpha = \frac{1}{r} \sum_{i=1}^{r} \xi_i^\alpha$ for $\alpha \in \mathbb{N}^n$. and by applying the method described in Section 2, we obtain a basis B of $\mathcal{A}_\sigma$, and a border basis with respect to B generating the vanishing ideal I_σ.

3.3. **Tensor decomposition.** We consider an homogeneous polynomial $T(x_0, \dots, x_n) \in \mathbb{K}[x_0, \dots, x_n]$ of degree $d \in \mathbb{N}$. The (symmetric) tensor decomposition problem consists in finding the least number r of linear forms $l_1, \dots, l_r$ and non-zero weights $\omega_1, \dots, \omega_r \in \mathbb{K}$ such that

$$T(x_0, \dots, x_n) = \sum_{i=1}^{r} \omega_i l_i (x_0, \dots, x_n)^d. \tag{3}$$

The problem of decomposition of T can be reformulated as the problem of decomposing a series $\sigma(\mathbf{z})$ as a sum of exponential polynomials, when the first coefficients σ_α ($|\alpha| \leqslant d$) are known. See [3, 2].

References

[1] M. Abril Bucero and B. Mourrain. Border Basis relaxation for polynomial optimization. http://hal.inria.fr/hal-00981546.

[2] A. Bernardi, J. Brachat, P. Comon, and B. Mourrain. General Tensor Decomposition, Moment Matrices and Applications. *Journal of Symbolic Computation*, 52(May):51–71, May 2013.

[3] J. Brachat, P. Comon, B. Mourrain, and E. Tsigaridas. Symmetric tensor decomposition. *Linear Algebra and Applications*, 433:1851–1872, 2010.

[4] Baron Gaspard Riche de Prony. Essai expérimental et analytique: sur les lois de la dilatabilité de fluides élastique et sur celles de la force expansive de la vapeur de l'alcool, à différentes températures. *J. Ecole Polyt.*, 1:24–76, 1795.

[5] M. Elkadi and B. Mourrain. *Introduction à la résolution des systèmes polynomiaux*, volume 59 of *Mathématiques & Applications (Berlin) [Mathematics & Applications]*. Springer, Berlin, 2007.

[6] J.-B. Lasserre, M. Laurent, B. Mourrain, P. Rostalski, and P. Trébuchet. Moment matrices, border bases and real radical computation. *J. Symbolic Comput.*, 51:63–85, 2013.

[7] M. Laurent and B. Mourrain. A generalized flat extension theorem for moment matrices. *Arch. Math. (Basel)*, 93(1):87–98, July 2009.

Inria Sophia Antipolis Méditerranée
E-mail address: Bernard.Mourrain@inria.fr

TRIANGULACIONES UNIMODULARES DE POLITOPOS RETICULARES

FRANCISCO SANTOS

ABSTRACT. We review recent and not-so-recent results about unimodular triangulations of lattice polytopes, and their relation to commutative algebra and (toric) algebraic geometry. In particular, we report on a new proof of the classical result by Kempf, Knudsen, Mumford and Saint-Donat (1973) saying that for every lattice polytope P there is a certain dilation factor c such that cP admits a regular unimodular triangulation.

A *lattice polytope* is a polytope with integer vertices (or with vertices lying in a point lattice). Put differently, it is the convex hull of a finite set of integer points in Euclidean space. A d-polytope is a polytope of dimension d. A *triangulation* (decomposition into simplices that intersect properly) of a lattice polytope is unimodular if all simplices are unimodular with respect to the lattice, that is, if their vertex sets are affine lattice bases.

Unimodularly triangulating a lattice polytope has applications ranging from Enumerative Combinatorics, to Integer Programming, to Algebraic Geometry. Sometimes the triangulations are required or seeked with additional properties, such as being regular and/or flag.

For example, let P be a lattice d-polytope, and identify P with $P \times \{1\} \subset \mathbb{R}^{d+1}$. Let σ_P be the polyhedral cone generated by $P \times \{1\}$. Then:

- Commutative algebraic properties of the graded semigroup ring $R_P = \mathbb{K}[\sigma_P \cap \mathbb{Z}^{d+1}]$ can be related to properties of the lattice points in P. For example, if every lattice point in $k \cdot P$ decomposes as the sum of k lattice points in P then R_P is generated by its elements of degree one. If this happens we say that P is an *integrally closed polytope*, and a sufficient condition for it is that it has a unimodular triangulation (in fact, it is enough if P has a *unimodular cover*; that is, if it can be expressed as a union of unimodular simplices).
- In turn, if P is integrally closed then the lattice points in P form a Hilbert basis for the set of integer points in σ_P, of interest in integer programming.
- The Hilbert series of R_P is nothing but the sequence counting the number of lattice points in the different dilations of P. In geometric combinatorics this is known as the Ehrhart series of P and its generating function can be always written as

$$\sum_{k\geq 0} \#(kP \cap \mathbb{Z}^d)\, t^k \;=\; \frac{h^*_P(t)}{(1-t)^{d+1}}\,,$$

  where $h^*_P(t)$ is a certain polynomial of degree $\leq d$. If P has a unimodular triangulation T, then h^* is nothing but the combinatorial h-polynomial of T, easily computable form the vector $(f_0, \dots, f_d)$ of faces of T of different dimensions.
- Associated to P and σ is also the affine toric variety

$$U_P = \operatorname{Spec} \mathbb{K}[\sigma_P^\vee \cap \mathbb{Z}^{d+1}],$$

where $\sigma_P^\vee$ is the cone dual to σ_P. U_P has a single singular point, at the origin (and is in fact a cone over this point). Resolutions of this singularity are closely related to unimodular triangulations of P. (More precisely, *crepant projective resolutions* of this singularity are in bijection to regular unimodular triangulations of P).

These crepant birational morphisms appear in the high-dimensional McKay correspondence for Gorenstein quotient singularities $\mathbb{C}^d/G$, proven by Batyrev.

Related to the latter item in the above list, one of the earliest, and to this day one of the most striking, results involving unimodular triangulations is the stable reduction theorem of Kempf, Knudsen, Mumford and Saint-Donat [2]. They showed that in characteristic zero, every one-dimensional family can be resolved so that the exceptional locus is a normal crossing divisor. They achieved this by reducing the statement to the case of "toroidal" singularities. The combinatorial core of the argument is the following result from [3]:

Theorem 0.1 (Knudsen-Mumford-Waterman [3]). *Let P be a lattice polytope. Then there is a $c \in \mathbb{N}$ such that $c \cdot P$ has a regular unimodular triangulation.*

In this statement a *regular* triangulation of P is one whose simplices are the domains of linearity of a convex and piecewise-affine function defined on P.

In this talk I will present several recent results on unimodular triangulations of lattice polytopes. The highlight is a new proof of the KMW Theorem stated above that includes a bound on the constant c. Our bound is doubly exponential in the dimension and the volume of P (of type $d^{d^{d^2 V}}$) but is an improvement over the original proof which did not come with an explicit bound. (and any bound derived from the original proof would involve a tower of exponentials of length related to the volume of P.

This is joint work with C. Haase, A. Paffenholz and L. Piechnik [1]. Some results about three-dimensional dilations are joint with Günder M. Ziegler [4].

References

[1] Christian Haase, Andreas Paffenholz, Lindsey C. Piechnik, and Francisco Santos, Existence of unimodular triangulations - positive results preprint May 2014, 82 pp. `http://arxiv.org/abs/1405.1687`

[2] George R. Kempf, Finn F. Knudsen, David Mumford, and Bernard Saint-Donat. *Toroidal Embeddings I*, volume 339 of *Lecture Notes in Mathematics*.
Springer–Verlag, 1973.

[3] Finn F. Knudsen. Construction of nice polyhedral subdivisions. In *Toroidal Embeddings I*, volume 339 of *Lecture Notes in Mathematics*, pages 109–164. Springer-Verlag, 1973. Chapter 3 of [2].

[4] Francisco Santos and Günter M. Ziegler. Unimodular triangulations of dilated 3-polytopes. *Trans. Moscow Math. Soc.*, 74:293–311, 2013.

Universidad de Cantabria
E-mail address: `francisco.santos@unican.es`

Contributed talks

NEW POLYNOMIAL OPTIMIZATION ALGORITHM USING BORDER BASIS

MARTA ABRIL BUCERO AND BERNARD MOURRAIN

ABSTRACT. A relaxation method based on border basis reduction which improves the efficiency of Lasserre's approach is proposed to compute the optimum of a polynomial function on a basic closed semi algebraic set. A new stopping criteria is given to detect when the relaxation sequence reaches the minimum, using a sparse flat extension criteria. We also provide a new algorithm to reconstruct a finite sum of weighted Dirac measures from a truncated sequence of moments, which can be applied to other sparse reconstruction problems. As an application, we obtain a new algorithm to compute zero-dimensional minimizer ideals and the minimizer points.

EXTEND ABSTRACT

Computing the global minimum of a polynomial function f on a semi-algebraic set is a difficult but important problem, with many applications. A relaxation approach was proposed in [6] which approximates this problem by a sequence of finite dimensional convex optimization problems. These optimization problems can be formulated in terms of linear matrix inequalities on moment matrices associated to the set of monomials of degree $\leq t \in \mathbb{N}$ for increasing values of t. They can be solved by Semi-Definite Programming (SDP) techniques. The sequence of minima converges to the actual minimum f^* of the function under some hypotheses [6]. In some cases, the sequence even reaches the minimum f^* in a finite number of steps [8, 16, 10, 2, 4, 14]. This approach proved to be particularly fruitful in many problems [7]. In contrast with numerical methods such as gradient descent methods, which converge to a local extremum but with no guaranty for the global solution, this relaxation approach can provide certificates for the minimum value f^* in terms of sums of squares representations.

From an algorithmic and computational perspective, some issues need however to be considered.

- *How to reduce the size of the moment matrices?* The size of the SDP problems to be solved is a bottleneck of the method. This size is related to the number of monomials of degree $\leq t$ and is increasing exponentially with the number of variables and the degree t. Many SDP solvers are based on interior point methods which provide an approximation of the optimal moment sequence within a given precision in a polynomial time [13]. Thus reducing the size of the moment matrices or the number of parameters can improve significantly the performance of these relaxation methods. We address this issue using polynomial reduction with border basis due to their numerical stability [11, 12].
- *When is the minimum reached?* A new stopping criteria is given to detect when the relaxation sequence reaches the minimum, using a flat extension criteria from [9]. We also provide a new algorithm to reconstruct a finite sum of weighted Dirac measures from a truncated sequence of moments. This reconstruction method can be used in other problems such as tensor decomposition [1] and multivariate sparse interpolation [3]

- *How to recover the minimizer ideal?* Computing the points where this minimum is reached if they exist, is critical in many applications. Determining when and how these minimizer points can be computed from the relaxation sequence is a problem that has been adressed for instance in [5, 15] using of kernel of full moment matrices

We present a new algorithm to obtain the minimum of a real polynomial function f in a semialgebraic set $G = (G^0, G^+)$ where G^0 is a set of equalities and G^+ is a set of inequalities non negatives and we suppose that the numbers of minimizer points is finite. We compare our algorithm with the full moment matrix relaxation algorithm (implemented in c++ in the same environment that our algorithm) described in [7], which is also implemented in the package Gloptipoly of Matlab developed by D. Henrion and J.B. Lasserre.

When there are equality constraints, the border basis computation reduces the size of the moment matrices, as well as the localization matrices associated to the inequalities. This speeds up the SDP computation. In the case where there are only inequalities, the size of the moments matrices is the same but the algorithm which verifies the flat extension and the algorithm which computes the minimizers are more efficient and quicker than the reconstruction algorithm used in the full moment matrix relaxation approach. The performance is not the only issue: numerical problems can also occur due to the bigger size of the moment matrices in the flat extension test and the reconstruction of minimizers.

The experiments show that when the size of the SDP problems becomes significant, most of the time is spent during `sdpa` computation and the border basis time and reconstruction time are negligible. In all the examples, the new border basis relaxation algorithm outperforms the full moment matrix relaxation method.

References

[1] J. Brachat, P. Comon, B. Mourrain, and E. Tsigaridas. Symmetric tensor decomposition. *Linear Algebra and Applications*, 433:1851–1872, 2010.

[2] J. Demmel, J. Nie, and V. Powers. Representations of positive polynomials on noncompact semialgebraic sets via kkt ideals. *Journal of Pure and Applied Algebra*, 209(1):189 – 200, 2007.

[3] M. Giesbrecht, G. Labahn, and W.-S. Lee. Symbolic-numeric sparse interpolation of multivariate polynomials. *J. Symb. Comput.*, 44(8):943–959, August 2009.

[4] H. V. Ha and T.S. Pham. Representation of positive polynomials and optimization on noncompact semialgebraic sets. *SIAM Journal on Optimization*, 20(6):3082–3103, 2010.

[5] D. Henrion and J.B. Lasserre. *Positive Polynomials in Control*, chapter Detecting Global Optimality and Extracting Solutions in GloptiPoly., pages 293–310. Lectures Notes in Control and Information Sciences. Springer, 2005.

[6] J.B. Lasserre. Global optimization with polynomials and the problem of moments. *SIAM J. Optim.*, 11:796–817, 2001.

[7] J.B Lasserre. *Moments, positive polynomials and their applications.* Imperial College Press, 210.

[8] M. Laurent. Semidefinite representations for finite varieties. *Math. Progr*, 109:1–26, 2007.

[9] M. Laurent and B. Mourrain. A generalized flat extension theorem for moment matrices. *Arch. Math. (Basel)*, 93(1):87–98, July 2009.

[10] M. Marshall. Representations of non-negative polynomials, degree bounds and applications to optimization. *Can. J. Math.*, 61(1):205–221, 2009.

[11] B. Mourrain and P. Trébuchet. Generalized normal forms and polynomials system solving. In M. Kauers, editor, *ISSAC: Proceedings of the ACM SIGSAM International Symposium on Symbolic and Algebraic Computation*, pages 253–260, 2005.

[12] B. Mourrain and Ph. Trébuchet. Stable normal forms for polynomial system solving. *Theoretical Computer Science*, 409(2):229–240, 2008.

[13] Y. Nesterov and A. Nemirovski. *Interior-point polynomial algorithms in convex programming*. SIAM, Philaldelphia, 1994.

[14] J. Nie. An exact jacobian SDP relaxation for polynomial optimization. *Mathematical Programming*, pages 1–31, 2011.

[15] J. Nie. Certifying convergence of Lasserre's hierarchy via flat truncation. *Mathematical Programming*, pages 1–26, 2012.

[16] J. Nie, J. Demmel, and B. Sturmfels. Minimizing polynomials via sum of squares over gradient ideal. *Math. Program.*, 106(3):587–606, 2006.

EPI GALAAD, INRIA MÉDITERRANÉE, BP 93, 06902 SOPHIA ANTIPOLIS, FRANCE
E-mail address: {Marta.Abril_Bucero,Bernard.Mourrain}@inria.fr

COMPUTING JUMPING NUMBERS AND MULTIPLIER IDEALS IN TWO-DIMENSIONAL REGULAR LOCAL RINGS

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

ABSTRACT. We give a new algorithm that computes the jumping numbers with their multiplicities and multiplier ideals of any ideal in a regular two-dimensional local ring.

INTRODUCTION

Multiplier ideals and jumping numbers are invariants associated to ideals which encode relevant information about their structure. When dealing with 2-dimensional local regular rings, as it is the case of this note, the jumping numbers and multiplier ideals of a fixed ideal are determined by the divisors appearing in the resolution of the ideal.

Recently, several authors provided formulae to compute the jumping numbers for complete ideals of 2-dimensional local regular rings. In the case of irreducible plane curves and simple complete ideals, Järvilehto [6] and Naie [9] give closed formulae to compute the jumping numbers. For complete ideals and multibranched curves, Tucker [11] presents an algorithm to compute the set of jumping numbers. In the case of the smallest jumping number, the so called log-canonical threshold, is given by Kuwata [7] and Galindo, Hernando and Monserrat [5].

This note presents a new algorithm, which computes the jumping numbers and multiplier ideals of any ideal or plane curve, through a completely different approach from Tucker's one. This algorithm computes the jumping numbers in any desired interval in a sequential way: starting from a jumping number, it computes the jumping numbers immediately after it (by the increasing ordering in the real line) and, these new jumping numbers are is achieved directly by computing a minimum among a finite set of rational numbers.

1. BASICS

This first part introduces the notions of multiplier ideal, jumping number and multiplicity and some basic properties that will be useful in the forthcoming sections.

Let X be a smooth complex surface of dimension two and $\mathcal{O}_{X,O}$ the ring of germs of holomorphic functions in a neighbourhood of a smooth point $O \in X$, for example, one can consider $X = \mathbb{C}^2$ and $\mathcal{O}_{X,O} = \mathbb{C}\{\{x,y\}\}$. If the point O is clear from the context, $\mathcal{O}_{X,O}$ will be denoted simply as $\mathcal{O}_X$.

Let $\mathfrak{a} \subseteq \mathcal{O}_X$ be an $\mathfrak{m}$-primary ideal different from zero and $c \in \mathbb{Q}_{>0}$. Let $\pi : X' \to X$ be a log-resolution of the ideal $\mathfrak{a}$, K_π the relative canonical divisor of the resolution and F the divisor defined as $\mathfrak{a} \cdot \mathcal{O}_{X'} = \mathcal{O}_{X'}(-F)$. The *multiplier ideal* associated to $\mathfrak{a}$ and c is

$$\mathcal{J}(\mathfrak{a}^c) = \pi_* \mathcal{O}_{X'}(K_\pi - \lfloor cF \rfloor).$$

It is worth to notice that, for all $c \in \mathbb{Q}$, $\mathcal{J}(\mathfrak{a}^c)$ is a complete ideal, and moreover, $\mathcal{J}(\mathfrak{a}^c) = \mathcal{J}(\bar{\mathfrak{a}}^c)$.

The set of all λ_i's, with $0 < \lambda_1 < \lambda_2 < ...$ such that $\mathcal{J}(\mathfrak{a}^c) = \mathcal{J}(\mathfrak{a}^{\lambda_i})$ for $c \in [\lambda_i, \lambda_{i+1})$ and $\mathcal{J}(\mathfrak{a}^{\lambda_{i+1}}) \subsetneq \mathcal{J}(\mathfrak{a}^{\lambda_i})$ for each i that form a nested sequence of ideals:

$$\mathcal{O}_X \supsetneq \mathcal{J}(\mathfrak{a}^{\lambda_1}) \supsetneq \mathcal{J}(\mathfrak{a}^{\lambda_2}) \supsetneq ... \supsetneq \mathcal{J}(\mathfrak{a}^{\lambda_i}) \supsetneq ...$$

are known as *jumping numbers*. Applying Skoda's Theorem (see [8, Theorem 9.6.21]), it is enough to compute the jumping numbers in the interval $(0, 2]$ for the case of complete ideals and, when dealing with curves, it is enough to compute them in the interval $(0, 1)$.

The first jumping number, λ_1, is called *log-canonical threshold*. Järvilehto [6] generalizes this definition to the notion of log-canonical threshold of an ideal $\mathfrak{a}$ with respect to another ideal $\mathfrak{b}$:

$$\lambda_{\mathfrak{b}} = \lambda_{\mathfrak{b}}^{\mathfrak{a}} = \inf\{\lambda \in \mathbb{Q}_{>0} \quad | \quad \mathfrak{b} \nsubseteq \mathcal{J}(\mathfrak{a}^c)\}.$$

In addition, he proves that the set of jumping numbers coincides with the set of log-canonical thresholds of $\mathfrak{a}$ with respect to another ideal.

Due to the fact that $\mathfrak{a}$ is an $\mathfrak{m}$-primary complete ideal, its associated multiplier ideals $\mathcal{J}(\mathfrak{a}^c)$ are also $\mathfrak{m}$-primary ideals. Allowing to consider their codimension as $\mathbb{C}$-vector spaces. The *multiplicity* of λ_i as jumping number is the codimension as $\mathbb{C}$-vector space of $\mathcal{J}(\mathfrak{a}^{\lambda_i})$ in $\mathcal{J}(\mathfrak{a}^{\lambda_{i-1}})$.

2. Tucker's algorithm

This section introduces Tucker's algorithm [11] which computes the jumping numbers of an ideal using the notion of critical contribution. Given two consecutive multiplier ideals $\mathcal{J}(\mathfrak{a}^{\lambda_{i-1}}) \supsetneq \mathcal{J}(\mathfrak{a}^{\lambda_i})$, we define a **critical divisor** G **associated to** λ_i as the reduced divisor that detects a jump minimally:

$$\mathcal{J}(\mathfrak{a}^{\lambda_{i-1}}) \supseteq \pi_* \mathcal{O}_{X'}(K_\pi - \lfloor \lambda_i F \rfloor + G) \supsetneq \mathcal{J}(\mathfrak{a}^{\lambda_i}) \,.$$

Moreover, λ is said to be a *candidate jumping number* for some divisor G, if $ord_{E_i}(K_\pi - \lambda F)$ is an integer for all prime divisors $E_i \leqslant G$. Using this notions, Tucker gives the following algorithm:

Algorithm 2.1 (Tucker, 2010). `Input :` $\mathfrak{a} \subseteq \mathcal{O}_{X,O}$.
`Output :` List of Jumping Numbers of $\mathfrak{a}$.

(1) Compute the set of all candidate jumping numbers.
(2) Find all possible critical divisors using a criterion that he provides in his article (see [11]).
(3) Find which candidate jumping numbers can be realized as jumping number associated to a critical divisor.

It is worth to point out that this algorithm also works when the surface X has rational singularities.

3. An algorithm to compute the jumping numbers and multiplier ideals

This section describes an algorithm that computes sequentially the chain of multiplier ideals:

$$\mathcal{O}_X \supsetneq \mathcal{J}(\mathfrak{a}^{\lambda_1}) \supsetneq \mathcal{J}(\mathfrak{a}^{\lambda_2}) \supsetneq ... \supsetneq \mathcal{J}(\mathfrak{a}^{\lambda_j}) \supsetneq ...$$

Namely, given any jumping number λ_{j-1}, the algorithm provides its associated multiplier ideal $\mathcal{J}(\mathfrak{a}^{\lambda_{j-1}})$, computes the next jumping number λ_j simply as a minimum of a finite set of rational numbers and repeats the process. The main advantage of this algorithm with respect to Tucker's algorithm is that it avoids computing of all the candidate jumping numbers and possible critical divisors.

To describe the multiplier ideal we will use the equivalence between $\mathfrak{m}$-primary complete ideals and antinef divisors. In general, the divisor $K_\pi - \lfloor \lambda F \rfloor$ is not antinef, but thanks to the *unloading* procedure described in [3, Section 4.6.], one can construct, the unique antinef divisor D_λ satisfying:

$$\mathcal{J}(\mathfrak{a}^\lambda) = \pi_* \mathcal{O}_{X'}(K_\pi - \lfloor \lambda F \rfloor) = \pi_* \mathcal{O}_{X'}(-D_\lambda)\,.$$

Let $\mathfrak{a} \subseteq \mathcal{O}_X$ be an $\mathfrak{m}$-primary ideal such that $\mathfrak{a} \cdot \mathcal{O}_{X'} = \mathcal{O}_{X'}(-F)$ with $F = \sum e_i E_i$ being an effective divisor, and $K_\pi = \sum_i k_i E_i$ be the relative canonical divisor.

Theorem 3.1. *Let λ_{j-1} be a jumping number of an $\mathfrak{m}$-primary ideal $\mathfrak{a} \subseteq \mathcal{O}_X$, such that $\mathfrak{a} \cdot \mathcal{O}_{X'} = \mathcal{O}_{X'}(-F)$ with $F = \sum e_i E_i$ being an effective divisor. Let $D_{\lambda_{j-1}} = \sum e_i^{\lambda_{j-1}} E_i$ be the antinef closure of $K_\pi - \lfloor \lambda_{j-1} F \rfloor$. Then,*

$$\lambda_j = \min_i \left\{ \frac{k_i + 1 + e_i^{\lambda_{j-1}}}{e_i} \right\}$$

is the jumping number consecutive to λ_{j-1}.

This theorem allows us to give the following algorithm to compute the jumping numbers and multiplier ideals:

Algorithm 3.2. `Input` **:** Weighted cluster of base points of $\mathfrak{a} \subseteq \mathcal{O}_{X,O}$.
`Output` **:** List of jumping numbers of $\mathfrak{a}$ and its corresponding multiplier ideals and their multiplicities.
For j from 1 to s (until $\lambda_s = 1$ in case of curves and $\lambda_s = 2$ for ideals), incrementing by 1
(Step j)

- **Jumping number**: Compute

$$\lambda_j = \min_i \left\{ \frac{k_i + 1 + e_i^{\lambda_{j-1}}}{e_i} \right\}.$$

- **Multiplier ideal**: Compute the antinef closure D_{λ_j} of $K_\pi - \lfloor \lambda_j F \rfloor$ using the unloading procedure.

Moreover, rewriting proposition 4.7.1 of Casas-Alvero in [3] in terms of divisors, one can compute easily the multiplicity $m(\lambda_j)$ of the jumping number using the following formula:

$$m(\lambda_j) = \frac{D_{\lambda_j}(D_{\lambda_j} + K_\pi)}{2} - \frac{D_{\lambda_{j-1}}(D_{\lambda_{j-1}} + K_\pi)}{2}$$

The main difference between this algorithm and Tucker's algorithm is the way to find jumping numbers. In this method, each jumping number is computed as the log-canonical threshold with respect to the multiplier ideal associated to the previous jumping number. In addition, this algorithm gives as output not only the jumping numbers, but the associated multiplier ideals as well. It is worth to point out that one can extend Tucker's algorithm in order to compute the multiplier ideal associated to each jumping number using the unloading procedure.

Both algorithms have been implemented in Macaulay2. The proposed algorithm is faster than the extended version of Tucker's algorithm, since we do not need to find all the possible critical divisors. For example, we have tested the case of an $\mathfrak{m}$-primary ideal $\mathfrak{a}$ with 56986 jumping numbers in the interval $(0, 2]$. Using Tucker's algorithm it takes 4360.2 seconds to compute them all but the proposed algorithm method needs only 2559.01 seconds. That is, roughly speaking 30 minutes faster.

References

[1] M. Alberich-Carramiñana, J.Àlvarez-Montaner and F. Dachs-Cadefau, *Multiplier ideals in two-dimensional regular local rings*, Preprint

[2] M. Alberich-Carramiñana, J.Àlvarez-Montaner, F. Dachs-Cadefau and V. González-Alonso, *Poincaré series of multiplier ideals in two-dimensional regular local rings*, Preprint

[3] E. Casas-Alvero, *Singularities of plane curves*, London Math. Soc. Lecture Note Series, **276**, Cambridge University Press, Cambridge, 2000.

[4] L. Ein, R. Lazarsfeld, K. Smith and D. Varolin, *Jumping coefficients of multiplier ideals*, Duke Math. J. **123** (2004), 469–506.

[5] C. Galindo, F. Hernando and F. Monserrat, *The log-canonical threshold of a plane curve*, Preprint available at arXiv:1211.6274.

[6] T. Järviletho, *Jumping numbers of a simple complete ideal in a two-dimensional regular local ring*, Mem. Amer. Math. Soc. **214** (2011), no. 1009, viii+78 pp.

[7] T. Kuwata, *On log canonical thresholds of reducible plane curves*, Amer. J. Math. **121** (1999), 701–721.

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

[9] D. Naie, *Jumping numbers of a unibranch curve on a smooth surface*, Manuscripta Math. **128** (2009), 33–49.

[10] K. E. Smith and H. Thompson, *Irrelevant exceptional divisors for curves on a smooth surface*. in: Algebra, geometry and their interactions, Contemp. Math. **448** (2007), 245–254.

[11] K. Tucker, *Jumping numbers on algebraic surfaces with rational singularities*, Trans. Amer. Math. Soc. **362** (2010), 3223–3241.

Dept. Matemàtica Aplicada I
Univ. Politècnica de Catalunya
Av. Diagonal 647, Barcelona 08028, Spain
E-mail address: Maria.Alberich@upc.edu, Josep.Alvarez@upc.edu, Ferran.Dachs@upc.edu

HILBERT'S NULLSTELLENSATZ AND POLYNOMIAL DYNAMICAL SYSTEMS

CARLOS D'ANDREA, ALINA OSTAFE, IGOR E. SHPARLINSKI, AND MARTÍN SOMBRA

ABSTRACT. We use an explicit form of Hilbert's Nullstellensatz to estimate the largest prime and the number of primes p such that a reduction modulo p of a zero dimensional variety over $\mathbb{Q}$ becomes of positive dimension. We apply these estimates to studying cyclic points of polynomial dynamical systems in finite fields.

1. INTRODUCTION

Let $\mathbb{F}$ be an arbitrary field and

$$\mathcal{F} = \{F_1, \ldots, F_m\}, \qquad F_1, \ldots, F_m \in \mathbb{Z}[X_1, \ldots, X_m], \tag{1}$$

a system of be m polynomials in m variables over $\mathbb{Z}$. For each $i = 1, \ldots, m$ we define the k-th iteration of the rational function F_i by the recurrence relation

$$F_i^{(0)} = X_i, \quad F_i^{(n)} = F_i\left(F_1^{(n-1)}, \ldots, F_m^{(n-1)}\right), \quad n = 1, 2, \ldots, \tag{2}$$

see [2, 12, 13] for a background on dynamical systems associated with such iterations.

Given a vector $\mathbf{u} \in \mathbb{C}^m$ over the complex numbers, we define the orbit of $\mathbf{u}$, which we denote by $\mathcal{O}_{\mathcal{F},\mathbf{u}}$, as the sequence of vectors $\mathbf{u}_n = (u_{n,1}, \ldots, u_{n,m}) \in \mathbb{C}^m$ defined by the recurrence relation

$$u_{n+1,i} = F_i(u_{n,1}, \ldots, u_{n,m}), \qquad n = 0, 1, \ldots, \quad i = 1, \ldots, m,$$

with $\mathbf{u}_0 = \mathbf{u}$. Sometimes we also write

$$\mathbf{u}_n = \mathcal{F}^{(n)}(\mathbf{u}).$$

We say that $\mathbf{u}$ is a periodic point of the polynomial system (1) of order $k \ge 1$ if $\mathbf{u}_n = \mathbf{u}_{n+k}$ for every $n = 0, 1, \ldots$. We note that it is convenient for us not to request that k is the smallest positive integer with this property (that is, a periodic point of order k is also a periodic point of order $k\ell$ for any integer $\ell \ge 1$).

Given a prime p we extend the above definitions in a natural way to periodic points modulo p. We refer to [1, 3, 8, 11, 14] for recent advances in the study of periodic points and period lengths in reductions of orbits of dynamical systems modulo distinct primes. In fact most of our motivation comes from the recently introduced idea of transferring the Hasse principle for periodic points and thus linking local and global periodicity properties, see [15]. Here we show that an explicit form of Hilbert's Nullstellensatz provides a powerful tool which may produce various results in this direction.

2. Number of points on modular reductions of varieties

Here we use several algebraic geometry tools, such as an explicit version of *Hilbert's Nullstellensatz,* see [5, 9], to obtain new results about periodic points in reductions of polynomial dynamical systems.

Our approach is based on several new results about the number of points on reductions modulo primes of an algebraic variety, defined by polynomials over $\mathbb{Z}$, that has only finitely many zeros over $\mathbb{C}$. Namely, we show that for a sufficiently large prime p, such a variety $V/\mathbb{C}$ also has finitely many zeros over the algebraic closure $\overline{\mathbb{F}}_p$ of the finite field $\mathbb{F}_p$ of p elements.

Given a polynomial $F \in \mathbb{Z}[X_1, \ldots, X_m]$, we define its height, denoted $\mathrm{h}(F)$, as the logarithm of the maximum of the absolute values of its coefficients. Using *Chow forms* and an explicit version of Hilbert's Nullstellensatz, given in [5], we derive:

Theorem 2.1. *Let $F_1, \ldots, F_m \in \mathbb{Z}[X_1, \ldots, X_m]$ be polynomials of degree at most d and of height at most h. Assume that the zero set of $F_1, \ldots, F_m$ in $\mathbb{C}^m$ has a finite number T of distinct points. Then there exists $\mathfrak{A} \in \mathbb{N}$ with*

$$\log \mathfrak{A} \le (10m + 4)d^{2m-1}h + (54m + 98)d^{2m} \log(2m + 5)$$

such that, if p is a prime not dividing $\mathfrak{A}$, then the zero set of $F_1, \ldots, F_m$ in $\overline{\mathbb{F}}_p^m$ has at most T points.

Clearly, there are at most $O(\log \mathfrak{A}) = O(d^{2m-1}h + d^{2m})$ primes $p \mid \mathfrak{A}$ (where the impplied constant depends only on m).

We also recall that by the *Bézout theorem*, if T is finite then $T \le d^m$.

3. Periodic points and orbit intersections of polynomial dynamical systems

Estimating the growth of height and the degrees of the iterations of polynomial systems, we show that Theorem 2.1 yields:

Theorem 3.1. *Let $F_1, \ldots, F_m \in \mathbb{Z}[X_1, \ldots, X_m]$ be polynomials of degree at most d and of height at most h. Assume that a polynomial system* (1) *has finitely many periodic points of order k over $\mathbb{C}$. Then there exists an integer $\mathfrak{A}_k \ge 1$ with*

$$\log \mathfrak{A}_k \le (10m + 4)d^{k(2m-1)} \frac{d^k - 1}{d - 1} h + (54m + 98)d^{2km} \log(2m + 5)$$

such that, if p is a prime number not dividing $\mathfrak{A}_k$, then the reduction of $\mathcal{F}$ modulo p has at most

$$N_k(p) \le d^{km}$$

periodic points of order k.

Our next application is to frequency of orbit intersections of orbits of two polynomial systems. We note that in the univariate case, Ghioca, Tucker and Zieve [6, 7] proved that if two univariate nonlinear complex polynomials have an infinite intersection of their orbits, then they have a common iterate. Clearly such a result cannot hold in finite fields. Instead, we obtain an upper bound on the frequency of intersections.

Let $\mathcal{F}$ of the form (1) and consider another polynomial system

$$\mathcal{G} = \{G_1, \ldots, G_m\}, \qquad G_1, \ldots, G_m \in \mathbb{Z}[X_1, \ldots, X_m].$$

For two vectors $\mathbf{w} \in \mathbb{C}^m$, we denote by

$$\mathrm{Orb}_{\mathbf{w}}(\mathcal{F}) = \left\{ \mathcal{F}^{(n)}(\mathbf{w}) \mid n = 0, 1, \ldots \right\}$$

and similarly for $\mathrm{Orb}_{\mathbf{w}}(\mathcal{G})$.

We say that $\mathcal{F}$ and $\mathcal{G}$ have a *uniformly bounded synchronized orbit intersection over* $\overline{\mathbb{K}}$ if the size of the synchronised intersection of $\mathrm{Orb}_{\mathbf{w}}(\mathcal{F})$ and $\mathrm{Orb}_{\mathbf{w}}(\mathcal{G})$, that is, the size of the set

$$\mathfrak{I}_{\mathbf{w}}(\mathcal{F}, \mathcal{G}) = \{ \mathcal{F}^{(n)}(\mathbf{w}) = \mathcal{G}^{(n)}(\mathbf{w}) \mid n = 0, 1, \ldots \}$$

is uniformly bounded over all initial values $\mathbf{w} \in \overline{\mathbb{K}}^m$. That is, there is a constant L depending only on $\mathcal{F}$ and $\mathcal{G}$ so that for all initial values $\mathbf{w} \in \overline{\mathbb{K}}^m$,

$$\#\mathfrak{I}_{\mathbf{w}}(\mathcal{F}, \mathcal{G}) \le L. \tag{3}$$

Furthermore, if (3) holds we say that $\mathcal{F}$ and $\mathcal{G}$ have a *L-uniformly bounded synchronized orbit intersection over* $\overline{\mathbb{K}}$.

It turns out that for polynomial systems over $\mathbb{Z}$ with a uniformly bounded orbit intersection over $\overline{\mathbb{Q}}$, the orbits of their reductions modulo a prime p have a density of intersections at most $\varepsilon > 0$, provided that p does not divide a certain quantity depending only on $\varepsilon > 0$ (and the systems themselves).

Since the polynomial systems $\mathcal{F}$ and $\mathcal{G}$ are defined by polynomials over $\mathbb{Z}$, then for a prime p and an integer N, we can also define, for $\mathbf{u}, \mathbf{v} \in \overline{\mathbb{F}}_p^m$,

$$\mathfrak{I}_{\mathbf{u},\mathbf{v}}(\mathcal{F}, \mathcal{G}; p, N) = \left\{ \overline{\mathcal{F}}_p^{(n)}(\mathbf{u}) = \overline{\mathcal{G}}_p^{(n)}(\mathbf{v}) \mid n = 0, \ldots, N-1 \right\},$$

for some initial values $\mathbf{u}, \mathbf{v} \in \overline{\mathbb{F}}_p^m$, where $\overline{\mathcal{F}}_p$ and $\overline{\mathcal{G}}_p$ are the reductions of the polynomial systems $\mathcal{F}$ and $\mathcal{G}$ modulo p. Note that the quantity $\mathfrak{I}_{\mathbf{u},\mathbf{v}}(\mathcal{F}, \mathcal{G}; p, N)$ is defined in a more general situation for arbitrary initial points $\mathbf{u}, \mathbf{v} \in \overline{\mathbb{F}}_p^m$ while the uniform boundness is requested only for the same initial vector. However this distinction is not essential (as if two orbit intersect, after this intersection they can be considered as orbits originating from the same point). For instance, we obviously have

$$\max_{\mathbf{u},\mathbf{v} \in \overline{\mathbb{F}}_p^m} \#\mathfrak{I}_{\mathbf{u},\mathbf{v}}(\mathcal{F}, \mathcal{G}; p, N) \le 1 + \max_{\mathbf{w} \in \overline{\mathbb{F}}_p^m} \#\mathfrak{I}_{\mathbf{w},\mathbf{w}}(\mathcal{F}, \mathcal{G}; p, N).$$

Coupling an explicit version of Hilbert's Nullstellensatz from [5] with some combinatorial arguments we derive:

Theorem 3.2. *Let $\mathcal{F} = \{F_1, \ldots, F_m\}$ and $\mathcal{G} = \{G_1, \ldots, G_m\}$ be two polynomial systems of m polynomials from $\mathbb{Z}[X_1, \ldots, X_m]$ of degree at most d and of height at most h and with a L-uniformly bounded orbit intersection over $\overline{\mathbb{Q}}$. For any $\varepsilon > 0$ there exists $\mathfrak{B} \in \mathbb{N}$ with*

$$\log \mathfrak{B} \le M^{L+1} d^{(M-1)(L+1)m} \left(mh + (4m+8)\log(m+3) \right)$$

where $M = \lfloor 2\varepsilon^{-1}(L+2) \rfloor + 1$, such that, if p is a prime number not dividing $\mathfrak{B}$, then for any integer $N \ge M$, we have

$$\max_{\mathbf{u},\mathbf{v} \in \overline{\mathbb{F}}_p^m} \#\mathfrak{I}_{\mathbf{u},\mathbf{v}}(\mathcal{F}, \mathcal{G}; p, N) \le \varepsilon N.$$

ACKNOWLEDGEMENTS

The authors are very grateful to Dragos Ghioca, Luis Miguel Pardo, Thomas Tucker and Michael Zieve for many valuable discussions.

During the preparation of this work, D'Andrea was partially supported by the MICINN research project MTM2010-20279, Ostafe was by the Swiss National Science Foundation Grant PA00P2–139679, Shparlinski by the Australian Research Council Grant DP130100237, and Sombra by the MINECO research project MTM2012-38122-C03-02.

REFERENCES

[1] A. Akbary and D. Ghioca, 'Periods of orbits modulo primes', *J. Number Theory*, **129** (2009), 2831–2842.

[2] V. Anashin and A. Khrennikov, 'Applied algebraic dynamics', Walter de Gruyter, Berlin. 2009.

[3] R. L. Benedetto, D. Ghioca, B. Hutz, P. Kurlberg, T. Scanlon and T. J. Tucker, 'Periods of rational maps modulo primes', *Math. Ann.*, **355** (2013), 637–660.

[4] E. Bombieri and W. Gubler, *Heights in Diophantine geometry*, Cambridge Univ. Press, Cambridge, 2006.

[5] C. D'Andrea, T. Krick and M. Sombra, 'Heights of varieties in multiprojective spaces and arithmetic Nullstellensätze', *Annales Sci. de l'ENS* **46** (2013), 549-627.

[6] D. Ghioca, T. Tucker and M. Zieve, 'Intersections of polynomial orbits, and a dynamical Mordell-Lang conjecture', *Inventiones Math.*, **171** (2008), 463–483.

[7] D. Ghioca, T. Tucker and M. Zieve, 'Linear relations between polynomial orbits', *Duke Math. J.*, **161** (2012), 1379–1410.

[8] R. Jones, 'The density of prime divisors in the arithmetic dynamics of quadratic polynomials', *J. Lond. Math. Soc.*, **78** (2008), 523–544.

[9] T. Krick, L. M. Pardo, and M. Sombra, 'Sharp estimates for the arithmetic Nullstellensatz', *Duke Math. J.*, **109** (2001), 521–598.

[10] M. Mignotte, *Mathematics for computer algebra*, Springer-Verlag, Berlin, 1992.

[11] J. A. G. Roberts and F. Vivaldi, 'A combinatorial model for reversible rational maps over finite fields', *Nonlinearity*, **22** (2009), 1965–1982.

[12] K. Schmidt, *Dynamical systems of algebraic origin*, Progress in Math., v.128. Birkhäuser Verlag, Basel, 1995.

[13] J. H. Silverman, *The arithmetic of dynamical systems*, Springer, New York, 2007.

[14] J. H. Silverman, 'Variation of periods modulo p in arithmetic dynamics', *New York J. Math.*, **14** (2008), 601–616.

[15] A. Towsley, 'A Hasse principle for periodic points', *Intern. J. Number Theory*, **8** (2013), 2053–2068.

DEPARTAMENT D'ÀLGEBRA I GEOMETRIA, UNIVERSITAT DE BARCELONA. GRAN VIA 585, 08007 BARCELONA, SPAIN

E-mail address: cdandrea@ub.edu

SCHOOL OF MATHEMATICS AND STATISTICS, UNIVERSITY OF NEW SOUTH WALES, SYDNEY, NSW 2052, AUSTRALIA

E-mail address: alina.ostafe@unsw.edu.au

SCHOOL OF MATHEMATICS AND STATISTICS, UNIVERSITY OF NEW SOUTH WALES, SYDNEY, NSW 2052, AUSTRALIA

E-mail address: igor.shparlinski@unsw.edu.au

ICREA AND DEPARTAMENT D'ÀLGEBRA I GEOMETRIA, UNIVERSITAT DE BARCELONA. GRAN VIA 585, 08007 BARCELONA, SPAIN

E-mail address: sombra@ub.edu

THE CONFLUENT BEZOUT MATRIX

D. A. ARULIAH, R. M. CORLESS, G. M. DIAZ–TOCA, L. GONZALEZ–VEGA, AND A. SHAKOORI

ABSTRACT. The aim of this paper is to introduce the construction of the Bezout matrix of two univariate polynomials given by values in the Hermite interpolation basis, namely the confluent Bezout matrix. Moreover if such polynomials have exactly one common simple zero, we describe how to compute it from the null space of the confluent Bezout matrix. The paper continues the research on algebra by values initiated in [1] and [2], where the polynomials are presented in the Lagrange basis.

1. THE EXTENDED CONFLUENT BEZOUT MATRIX

Let $\mathbb{P}_d$ denote the vector space of univariate polynomials of degree at most d with coefficients in $\mathbb{C}$. Let $p(t)$, $q(t) \in \mathbb{P}_d$ with $d = \max(\deg(p), \deg(q))$. We begin with the construction of the Bezout matrix in the monomial basis from the Cayley quotient $C(t,\mu)$

$$C(t,\mu) = \frac{p(t)q(\mu) - p(\mu)q(t)}{t-\mu}. \tag{1}$$

The well known *Bezout matrix* of $p(t)$ and $q(t)$ in the monomial basis is the d by d symmetric matrix $\mathbf{B}_{\tilde{\boldsymbol{M}}} = [b_{ij}]$ of the coefficients of the Cayley quotient such that

$$C(t,\mu) = \boldsymbol{\Phi}^T_{\tilde{M}}(t)\mathbf{B}_{\tilde{\boldsymbol{M}}}\boldsymbol{\Phi}_{\tilde{M}}(\mu) = \sum_{i=1}^{d}\sum_{j=1}^{d} b_{ij}t^{i-1}\mu^{j-1}, \tag{2}$$

with $\boldsymbol{\Phi}_{\tilde{M}}(t) = \left[1, t, \ldots, t^{d-1}\right]^T$. Now assume that we do not have $p(t)$ and $q(t)$ expressed in the monomial basis but in the Hermite interpolation basis (see [6]). We are given N distinct nodes $\boldsymbol{\tau} = (\tau_1, \tau_2, \ldots, \tau_N)$ with positive integer confluencies $\boldsymbol{s} = (s_1, s_2, \ldots, s_N)$, $\sum_{k=1}^{N} s_k = d+1$, and the evaluations (including some of the derivatives) at the given nodes

$$\boldsymbol{p} = (p_1, \ldots, p_1^{(s_1-1)}, \ldots, p_N, \ldots, p_N^{(s_N-1)}), \boldsymbol{q} = (q_1, \ldots, q_1^{(s_1-1)}, \ldots, q_N, \ldots, q_N^{(s_N-1)}),$$

where $p_k^{(r)}$ is the rth derivative of $p(t)$ at τ_k. Then, $p(t)$ and $q(t)$ are represented as

$$p(t) = \sum_{k=1}^{N}\sum_{r=0}^{s_k-1} p_k^{(r)}\, h_{k,r}(t)\,, q(t) = \sum_{k=1}^{N}\sum_{r=0}^{s_k-1} q_k^{(r)}\, h_{k,r}(t)\,, \tag{3}$$

where the polynomials $h_{k,r}(t)$ define the Hermite interpolation basis in $\mathbb{P}_d$. In fact, the coefficients of the polynomials $h_{k,r}(t)$ are given by the inverse of the confluent Vandermonde matrix $\mathbf{V}_c(\boldsymbol{\tau}; \boldsymbol{s})$.

Definition 1.1. Let $\ell_k = s_k - 1$ where, $1 \leqslant k \leqslant N$. Then, the confluent Vandermonde matrix $\mathbf{V}_c$ is a $d+1$ by $d+1$ matrix

$$\mathbf{V}_c(\boldsymbol{\tau}; \boldsymbol{s}) = \begin{bmatrix} \mathbf{V}(\tau_1; s_1) \\ \vdots \\ \mathbf{V}(\tau_N; s_N) \end{bmatrix}, \tag{4}$$

where $\mathbf{V}(\tau_k; s_k)$ is a $s_k \times (d+1)$ block matrix of the form

$$\mathbf{V}(\tau_k; s_k) = \begin{bmatrix} 1 & \tau_k & \tau_k^2 & \dots & \tau_k^d \\ 0 & 1 & 2\tau_k & \dots & d\tau_k^{d-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & \frac{d!}{(d-s_k+1)!}\tau_k^{d-s_k+1} \end{bmatrix}. \tag{5}$$

Similar to the situation in the monomial basis, we can use the basis-independent construction of the Cayley quotient to define the Bezout matrix in the Hermite interpolation basis. Let $\boldsymbol{\Phi}_H(t; \boldsymbol{\tau}) = [h_{1,0}(t), \dots, h_{1,s_1-1}(t), \dots, h_{N,0}(t), \dots, h_{N,s_N-1}(t)]^T$.

Definition 1.2. The *extended confluent Bezout* matrix is given by the matrix of coefficients $\mathbf{B}_{\boldsymbol{H}}$ in $\mathbb{C}^{d+1 \times d+1}$ of the Cayley quotient in the Hermite basis for $\mathbb{P}_d$. That is,

$$C_{p,q}(t, \mu) = \boldsymbol{\Phi}_H^T(t; \boldsymbol{\tau}) \mathbf{B}_{\boldsymbol{H}} \boldsymbol{\Phi}_H(\mu; \boldsymbol{\tau}) = \sum_{i=1}^{d+1} \sum_{j=1}^{d+1} b_{i,j} H_i(t) H_j(\mu). \tag{6}$$

Thus, if

$$\mathbf{B}_{\boldsymbol{M}} = \begin{bmatrix} \mathbf{B}_{\tilde{\boldsymbol{M}}} & & 0 \\ & & \vdots \\ 0 & \dots & 0 \end{bmatrix}, \tag{7}$$

then, $\mathbf{B}_{\boldsymbol{H}} = \mathbf{V}_c(\boldsymbol{\tau}; \boldsymbol{s}) \mathbf{B}_{\boldsymbol{M}} \mathbf{V}_c^T(\boldsymbol{\tau}; \boldsymbol{s})$. Our main goal is to construct the Bezout matrix without converting the problem to the monomial basis. Theorem 1.3 is the key for this process but we need to introduce some concepts before.

- For $1 \leqslant i \leqslant d+1$, we define $k(i)$, $1 \leqslant k(i) \leqslant N$, to denote the node index.
- We introduce $r(i)$ to denote the orders of the derivative evaluations at the node $\tau_{k(i)}$.

Theorem 1.3. *The entries of the extended confluent Bezout matrix $\mathbf{B}_{\boldsymbol{H}}$ are as following.*

(1) *For $1 \leqslant i, j \leqslant d+1$, if $k(i) \neq k(j)$*

$$b_{i,j} = \sum_{\alpha=0}^{r(i)} \sum_{\beta=0}^{r(j)} (-1)^{r(i)+\alpha} \binom{r(i)}{\alpha} \binom{r(j)}{\beta} (r(i) + r(j) - (\alpha+\beta))!$$

$$\cdot \left(\frac{p_{k(i)}^{(\alpha)} q_{k(j)}^{(\beta)} - p_{k(j)}^{(\beta)} q_{k(i)}^{(\alpha)}}{(\tau_{k(i)} - \tau_{k(j)})^{r(i)+r(j)-(\alpha+\beta)+1}} \right) \tag{8}$$

(2) *For* $1 \leqslant i, j \leqslant d+1$, *if* $k(i) = k(j)$, *assuming* $d = \max(\deg p(t), q(t))$,

$$b_{i,j} = \sum_{\nu=r(i)+1}^{d} \sum_{\beta=0}^{r(i)+r(j)-\nu+1} (-1)^{v-r(i)-1} \cdot r(j)!$$

$$\cdot \frac{\left(p_{k(i)}^{(\nu+\beta)} q_{k(i)}^{(r(i)+r(j)-\nu-\beta+1)} - q_{k(i)}^{(\nu+\beta)} p_{k(i)}^{(r(i)+r(j)-\nu-\beta+1)}\right)}{\nu\beta!(r(i)+r(j)-\nu-\beta+1)!(\nu-r(i)-1)!}. \tag{9}$$

Proof. The main strategy is to apply the generalization of the Leibnitz's product rule. The details of the proof have been presented in [4]. For the entries which face division by zero (i.e., $t = \mu$) we replace the Taylor expansion of $p(t)$ and $q(t)$ about $t = \mu$. □

In [7] they present a Derivative Formula which allows us to compute the required values of the derivatives in Equation (9).

2. THE CONFLUENT BEZOUT MATRIX

Observe that the matrix $\mathbf{B}_{\boldsymbol{H}}$ is one dimension bigger than the desired Bezout matrix. To extract the Bezout matrix of the desired dimension, we must reduce a confluency by one and consider a new Hermite interpolation basis. We would like to point out that the one evaluation to be removed can only be the the last one.

Suppose that the confluency of the last node, s_N, is reduced by one. Let $\tilde{\boldsymbol{p}}$, $\tilde{\boldsymbol{q}}$, $\tilde{\boldsymbol{\tau}}$ and $\tilde{\boldsymbol{s}}$ denote the values corresponding to the reduced interpolation scheme. The Hermite basis of the reduced interpolation scheme corresponding to $\tilde{\boldsymbol{\tau}}$ and $\tilde{\boldsymbol{s}}$ is

$$\boldsymbol{\Phi}_H(t; \tilde{\boldsymbol{\tau}}) = \left[\tilde{H}_1(t), \tilde{H}_2(t), \ldots, \tilde{H}_d(t)\right]^T \in [\mathbb{P}_{d-1}]^d. \tag{10}$$

Since $C_{p,q}(t, \mu)$ is of degree at most $d-1$ in each variable, we can write as in Equation 6

$$C_{p,q}(t, \mu) = \boldsymbol{\Phi}_H^T(t; \tilde{\boldsymbol{\tau}}) \mathbf{B}_{\tilde{\boldsymbol{H}}} \boldsymbol{\Phi}_H(\mu; \tilde{\boldsymbol{\tau}}), \tag{11}$$

where the corresponding Bezoutian $\mathbf{B}_{\tilde{\boldsymbol{H}}}$ is a d by d matrix and verifies

$$\mathbf{B}_{\tilde{\boldsymbol{H}}} = \mathbf{V}_c(\tilde{\boldsymbol{\tau}}; \tilde{\boldsymbol{s}}) \mathbf{B}_{\tilde{\boldsymbol{M}}} \mathbf{V}_c^T(\tilde{\boldsymbol{\tau}}; \tilde{\boldsymbol{s}}).$$

Theorem 2.1. [4] *The confluent Bezoutian* $\mathbf{B}_{\tilde{\boldsymbol{H}}}$ *of Equation* (11), *constructed from the reduced Hermite interpolation scheme with* $\tilde{\boldsymbol{s}} = \{s_1, \ldots, s_N - 1\}$ *is the* d *by* d *upper left block matrix of the corresponding extended confluent Bezoutian* $\mathbf{B}_{\boldsymbol{H}}$.

Finally, let us mention that there is a direct connection between the null space of the Bezout matrix and the common roots (see [5]). For example, if $\gcd(p(t), q(t)) = t - t^*$, it is possible to compute the common root t^* as follows.

Proposition 2.2. [5] *Let* $1 = a_1\tilde{H}_1(t) + \ldots + a_d\tilde{H}_d(t)$, *and* $t = b_1\tilde{H}_1(t) + \ldots + b_d\tilde{H}_d(t)$. *If* $(u_1, u_2, \ldots, u_d)^t$ *is a non vanishing vector in the nullspace of* $\mathbf{B}_{\tilde{\boldsymbol{H}}}$, *then*

$$t^* = \frac{b_1u_1 + \ldots + b_du_d}{a_1u_1 + \ldots + a_du_d}. \tag{12}$$

Observe that the coordinates of 1 and t in the reduced Hermite interpolation basis are given by the first and second column of $\mathbf{V}_c(\tilde{\boldsymbol{\tau}};\tilde{\boldsymbol{s}})$ respectively. Moreover it is well know that the degree of the greatest common divisor is equal to the dimension of the null space. Thus, if such a dimension is equal to 1, it is possible to directly compute the common root.

Example 2.3. As input we have

$$\boldsymbol{\tau}=[1,2], \boldsymbol{s}=[3,2], \boldsymbol{p}=[24,53,18,77,45], \boldsymbol{q}=[8,-25,-10,-21,-32].$$

In this case, we consider $\boldsymbol{\tau}=\tilde{\boldsymbol{\tau}}$ and $\tilde{\boldsymbol{s}}=[3,1]$. The confluent Bezout matrix is equal to

$$\mathbf{B}_{\tilde{\boldsymbol{H}}}=\begin{bmatrix} 1024 & 192 & -208 & 1120 \\ 192 & -64 & 410 & 308 \\ -208 & 410 & 64 & 224 \\ 1120 & 308 & 224 & 1519 \end{bmatrix}$$

and the null space is spanned by the vector $\left(-\frac{511}{512},-\frac{63}{64},-\frac{7}{16},1\right)$. Then there is only one simple common root. By applying Proposition 2.2 with

$$1=1\cdot\tilde{H}_1+1\cdot\tilde{H}_4 \text{ and } t=1\cdot\tilde{H}_1+1\cdot\tilde{H}_2+2\cdot\tilde{H}_4,$$

we obtain $t^*=(-511/512-63/64+2)/(-511/512+1)=9$.

References

[1] R.M. Corless, G.M. Diaz-Toca, M. Fioravanti , L. Gonzalez-Vega, I. F. Rua and A. Shakoori. *Computing the topology of a real algebraic plane curve whose defining equations are available only "by values"*. Computer Aided Geometric Design 30, pages 675–706, 2013.

[2] G.M. Diaz-Toca, M. Fioravanti , L. Gonzalez-Vega and A. Shakoori. *Using implicit equations of parametric curves and surfaces without computing them: Polynomial algebra by values*. Computer Aided Geometric Design 30, pages 116–139, 2013.

[3] A. Shakoori.*The Bézout matrix in the Lagrange Basis*. Proceedings of EACA 2004, pages 295–299, 2004.

[4] A. Shakoori. *Bivariate Polynomial Solver by Values*. PhD Thesis, The University of Western Ontario, London, Ontario, 2007.

[5] M. Fioravanti and G.M. Diaz–Toca. *The nullspace of the Bezout matrix in any basis and gcd's*. Preprint, 2014.

[6] R.A. Horn, C.R. Johnson. *Topics in Matrix Analysis*. Cambridge University Press, Cambridge, 1991.

[7] W. Werner and C. Schneider. *Hermite Interpolation: The Barycentric Approach*, Computing 46, pages 35–51, 1991.

Institute of Technology, University of Ontario, Canada
E-mail address: Dhavide.Aruliah@uoit.ca

Department of Applied Mathematics, University of Western Ontario, Canada
E-mail address: rcorless@uwo.ca

Departamento de Matemática Aplicada, Universidad de Murcia, Spain
E-mail address: gemadiaz@um.es

Departamento de Matemáticas, Estadística y Computación, Universidad de Cantabria, Spain
E-mail address: laureano.gonzalez@unican.es

Faculty of Science, University of Ontario Institute of Technology, Canada
E-mail address: azar.shakoori@gmail.com

A SEMIGROUP APPROACH TO PROJECTIVE MONOMIAL CURVES ASSOCIATED TO ARITHMETIC SEQUENCES

I. BERMEJO, E. GARCÍA-LLORENTE, AND I. GARCÍA-MARCO

ABSTRACT. Let k be an infinite field and $m_1 < \cdots < m_n$ an arithmetic sequence. We consider the projective monomial curve $\mathcal{C} \subset \mathbb{P}_k^n$ parametrically defined by

$$x_1 = t^{m_1}s^{m_n-m_1}, \ldots, x_{n-1} = t^{m_{n-1}}s^{m_n-m_{n-1}}, x_n = t^{m_n}, x_{n+1} = s^{m_n}.$$

In this work, we obtain formulas for the Castelnuovo-Mumford regularity of $\mathcal{C}$ and for the Cohen-Macaulay type and the Hilbert series of its corresponding coordinate ring $k[\mathcal{C}]$. As a byproduct we characterize the Gorenstein property for $k[\mathcal{C}]$. These formulas are obtained by means of the study of the semigroup $\mathcal{S} \subset \mathbb{N}^2$ associated to $\mathcal{C}$. As a consequence, we also determine all the Frobenius vectors of $\mathcal{S}$.

INTRODUCTION

Let $R = k[x_1, \ldots, x_{n+1}]$ be the polynomial ring in $n+1$ variables over an infinite field k. A binomial in R is a difference of two monomials. An ideal of R generated by binomials is called a binomial ideal.

Let $m_1 < \cdots < m_n$ be positive integers and consider the projective monomial curve $\mathcal{C} \subset \mathbb{P}_k^n$ parametrically defined by

$$x_1 = t^{m_1}s^{m_n-m_1}, \ldots, x_{n-1} = t^{m_{n-1}}s^{m_n-m_{n-1}}, x_n = t^{m_n}, x_{n+1} = s^{m_n}.$$

Consider the k-algebra homomorphism $\varphi : R \to k[t,s]$ induced by $\varphi(x_i) = t^{m_i}s^{m_n-m_i}$ for $i \in \{1, \ldots, n\}$ and $\varphi(x_{n+1}) = s^{m_n}$. Since k is infinite, the prime ideal $\mathcal{P} := ker(\varphi) \subset R$ is the defining ideal of $\mathcal{C}$ (see, e.g., [7, Corollary 7.1.12]). Moreover, it is a homogeneous binomial ideal (see, e.g., [6, Lemmas 4.1 and 4.14]). The most important algebraic object associated to $\mathcal{C}$ is its coordinate ring $k[\mathcal{C}] = R/\mathcal{P}$.

The projective monomial curve $\mathcal{C}$ has associated a semigroup $\mathcal{S} \subset \mathbb{N}^2$ in a natural way. Namely, $\mathcal{S}$ is the subsemigroup of $\mathbb{N}^2$ generated by $a_1, \ldots, a_{n+1}$, where

$$a_1 := \begin{pmatrix} m_1 \\ m_n - m_1 \end{pmatrix}, \ldots, a_{n-1} := \begin{pmatrix} m_{n-1} \\ m_n - m_{n-1} \end{pmatrix}, a_n := \begin{pmatrix} m_n \\ 0 \end{pmatrix} \text{ and } a_{n+1} := \begin{pmatrix} 0 \\ m_n \end{pmatrix}.$$

Our aim is to study the projective monomial curve $\mathcal{C}$ and its corresponding coordinate ring $k[\mathcal{C}]$ via the semigroup $\mathcal{S}$ when $m_1 < \cdots < m_n$ is an arithmetic sequence, i.e., when $m_i = m_1 + (i-1)d$ for all $i \in \{1, \ldots, n\}$, $d \in \mathbb{Z}^+$; without loss of generality, we also assume that $\gcd\{m_1, \ldots, m_n\} = 1$. More precisely, we aim at obtaining formulas for the Castelnuovo-Mumford regularity of $\mathcal{C}$ and for the Cohen-Macaulay type and the Hilbert series of $k[\mathcal{C}]$. This work follows the strategy presented by Böhm, Eisenbud and Nitsche in [4], where the authors study semigroup rings by means of a particular subset of the corresponding semigroup.

The structure of this work is the following. The first section will be devoted to a thorough study the semigroup $\mathcal{S} \subset \mathbb{N}^2$. More precisely, we will complete describe the subset of $\mathcal{S}$ that will interest us in the sequel; namely,

$$\mathcal{B} := \{b \in \mathcal{S} \mid b - a_n \notin \mathcal{S} \text{ and } b - a_{n+1} \notin \mathcal{S}\}\,.$$

As a byproduct of the description of $\mathcal{B}$ we characterize the set of Frobenius vectors of $\mathcal{S}$.

In the second section we will use the description of $\mathcal{B}$ to get information about $\mathcal{C}$ and $k[\mathcal{C}]$. More precisely, following the results of [4], we will be able to prove that $\mathcal{C}$ is always Cohen-Macaulay and to provide a formula for the Castelnuovo-Mumford regularity of $\mathcal{C}$. Moreover, following the ideas of Cavaliere and Niesi [5], we will also be able to determine the Cohen-Macaulay type of $k[\mathcal{C}]$ and, as a consequence of this, we will characterize when $k[\mathcal{C}]$ is Gorenstein. Finally, we will also describe the bivariate Hilbert series of $k[\mathcal{C}]$.

1. The semigroup associated to $\mathcal{C}$

The aim of this section is the study of the semigroup $\mathcal{S} \subset \mathbb{N}^2$ we considered in the introduction when $m_1 < \cdots < m_n$ is an arithmetic sequence with $\gcd\{m_1, \ldots, m_n\} = 1$. The first result gives an explicit description of the set

$$\mathcal{B} := \{b \in \mathcal{S} \mid b - a_n \notin \mathcal{S} \text{ and } b - a_{n+1} \notin \mathcal{S}\}$$

in terms of the arithmetic sequence $m_1 < \cdots < m_n$.

Proposition 1.1.

$$\mathcal{B} = \left\{ \begin{pmatrix} k_i\, m_n - id \\ id \end{pmatrix} \mid 0 \leq i < m_n \text{ and } k_i = \left\lceil \frac{i}{n-1} \right\rceil \right\}$$

As a consequence of this result we are able to characterize the Frobenius vectors of the semigroup $\mathcal{S}$. Recall that $v \in \mathbb{Z}^2$ is a Frobenius vector of $\mathcal{S}$ if and only if $v \in \mathbb{Z}\mathcal{S}$, $v \notin \mathcal{S}$ and for every $w = (w_1, w_2) \in \mathbb{Z}\mathcal{S}$ with $w_1, w_2 > 0$, then $v + w \in \mathcal{S}$.

Theorem 1.2. *Set $q, r \in \mathbb{N}$ such that $m_1 - 1 = q(n-1) + r$ with $r \in \{1, \ldots, n-1\}$.*

(a) *If $r = 1$, then the set of Frobenius vectors of $\mathcal{S}$ is $\{v + \lambda a_n, v + \lambda a_{n+1} \mid \lambda \in \mathbb{N}\}$, where* $v := \begin{pmatrix} qm_n + d \\ dm_n - m_n - d \end{pmatrix} \in \mathbb{Z}^2$.

(b) *If $r \neq 1$, then the set of Frobenius vectors of $\mathcal{S}$ is $\{v_1 + \lambda a_n, v_2 + \lambda a_{n+1} \mid \lambda \in \mathbb{N}\}$, where* $v_1 := \begin{pmatrix} (q+1)m_n + d \\ dm_n - m_n - d \end{pmatrix} \in \mathbb{Z}^2$ *and* $v_2 := \begin{pmatrix} (q+d)m_1 - d \\ (q+d)(n-1)d + d \end{pmatrix} \in \mathbb{Z}^2$.

2. Properties of the curve $\mathcal{C}$

This section is devoted to the study of the curve $\mathcal{C}$. Firstly, since the set $\mathcal{B}$ described in Proposition 1.1 has exactly m_n elements, by [4, Proposition 3.1(2)], we directly get the following result.

Corollary 2.1. *$\mathcal{C}$ is an arithmetically Cohen-Macaulay curve.*

Now we focus on giving an explicit formula in terms of the arithmetic sequence for the *Castelnuovo-Mumford regularity*, or simply regularity, of the curve $\mathcal{C}$.

The *regularity* $\operatorname{reg}(\mathcal{C})$ of $\mathcal{C}$ is by definition the Castelnuovo-Mumford regularity $\operatorname{reg}(\mathcal{P})$ of $\mathcal{P}$. Recall that (see, e.g., [1]) if

$$0 \to \bigoplus_{j=1}^{\beta_p} R(-e_{pj}) \xrightarrow{\phi_p} \cdots \xrightarrow{\phi_1} \bigoplus_{j=1}^{\beta_0} R(-e_{0j}) \xrightarrow{\phi_0} \mathcal{P} \to 0 \tag{1}$$

is a minimal graded free resolution of $\mathcal{P}$, then

$$\operatorname{reg}(\mathcal{P}) := \max\{e_{ij} - i;\ 0 \le i \le p,\ 1 \le j \le \beta_i\}.$$

Since $\mathcal{C}$ is arithmetically Cohen-Macaulay, by [4, Proposition 4.1] we have that $\operatorname{reg}(\mathcal{C})$ can be computed as the maximum of $(b_1 + b_2)/m_n$ plus one, where $(b_1, b_2) \in \mathcal{B}$. Hence we deduce the following result.

Theorem 2.2. $\operatorname{reg}(\mathcal{C}) = \left\lceil \frac{m_n - 1}{n-1} \right\rceil + 1$

It is worth pointing out that in our previous work [2] we had already obtained this result by a different approach based on the description of a Gröbner basis of $\mathcal{P}$ with respect to the reverse lexicographic order and following the techniques of [3].

Now we will provide a formula for the Cohen-Macaulay type of $k[\mathcal{C}]$. Recall that whenever $k[\mathcal{C}]$ is Cohen-Macaulay, its Cohen-Macaulay type is the last Betti number in the minimal graded free resolution of $\mathcal{P}$, i.e., the value of β_p in (1). Moreover, in [5, Proposition (4.9)], the authors prove that the Cohen-Macaulay type of $k[\mathcal{C}]$ equals the number of elements in $\mathcal{B}$ that are maximal with respect $<$, where $x < y \Leftrightarrow y - x \in \mathcal{S}$. Hence, we get the following result.

Theorem 2.3. *Set $q, r \in \mathbb{N}$ such that $m_1 - 1 = q(n-1) + r$ with $r \in \{1, \ldots, n-1\}$. Then, the Cohen-Macaulay type of $k[\mathcal{C}]$ is r.*

Since $k[\mathcal{C}]$ is Gorenstein if and only if it is Cohen-Macaulay and has type one, one can easily deduce the following characterization of the Gorenstein property.

Corollary 2.4. *$k[\mathcal{C}]$ is Gorenstein $\Longleftrightarrow m_1 \equiv 2 \pmod{n-1}$.*

Finally, we provide an explicit description of the bivariate Hilbert series of $k[\mathcal{C}]$. Recall that, if we denote by $\mathbf{t}^b := t_1^{b_1} t_2^{b_2}$ for all $b = (b_1, b_2) \in \mathbb{N}$, the bivariate Hilbert series of $k[\mathcal{C}]$ is the formal power series $H_{k[\mathcal{C}]}(t_1, t_2) \in \mathbb{Z}[[t_1, t_2]]$ given by

$$H_{k[\mathcal{C}]}(t_1, t_2) := \textstyle\sum_{b \in \mathcal{S}} \mathbf{t}^b.$$

Again, as a consequence of Proposition 1.1, we get the following result.

Theorem 2.5. *Set $q, r \in \mathbb{N}$ such that $m_n - 1 = q(n-1) + r$ with $r \in \{1, \ldots, n-1\}$. Then,*

$$H_{k[\mathcal{C}]}(t_1, t_2) = \frac{1 + \sum_{i=2}^{n-1} \mathbf{t}^{a_i} - \mathbf{t}^{qa_1}(\sum_{i=1}^{n-r-1} \mathbf{t}^{a_j} + \sum_{i=n-r}^{n-1} \mathbf{t}^{a_1+a_i})}{(1-t_1^{m_n})(1-t_2^{m_n})(1-\mathbf{t}^{a_1})}.$$

REFERENCES

[1] D. Bayer & D. Mumford, What can be computed in algebraic geometry?, in: D. Eisenbud, L. Robbiano (Eds.), Computational Algebraic Geometry and Commutative Algebra, Proceedings Cortona 1991, Cambridge University Press (1993), 1–48.

[2] I. Bermejo, E. García-Llorente & I. García-Marco, Castelnuovo-Mumford regularity of projective monomial curves associated to arithmetic sequences, submitted.

[3] I. Bermejo & P. Gimenez, Saturation and Castelnuovo-Mumford regularity, J. Algebra **303** (2006), 592–617.

[4] J. Böhm, D. Eisenbud & M.J. Nitsche, Decomposition of Semigroup Algebras, Experimental Mathematics, **21** (2012), no. 4, 385–394.

[5] M.P. Cavaliere & G. Niesi, On monomial curves and Cohen-Macaulay type, Manuscripta Math., **42** (1983), no. 2-3, 147–159.

[6] B. Sturmfels, *Gröbner bases and convex polytopes*, University Lecture Series **8**, American Mathematical Society, Providence,1996.

[7] R.H. Villarreal, *Monomial Algebras*, Monographs and Textbooks in Pure and Applied Mathematics **238**, Marcel Dekker, New York, 2001.

Departamento de Matemática Fundamental. Facultad de Matemáticas. Universidad de La Laguna. 38200 La Laguna, Tenerife, Spain.

E-mail address: ibermejo@ull.es, evgarcia@ull.es

Unviersité Montpellier 2. Insitut de Mathématiques et de Modélistation de Montpellier (I3M). Place Eugène Bataillon. 34095 Montpellier Cedex, France.

E-mail address: ignacio.garcia-marco@univ-montp2.fr

THE SCHEME OF LIFTINGS AND APPLICATIONS

C. BERTONE, F. CIOFFI, M. GUIDA, AND M. ROGGERO

ABSTRACT. We study the locus of the x_n-liftings of a homogeneous ideal H in a polynomial ring over a field K. We prove that this locus can be endowed with a structure of scheme in a constructive way, using Gröbner bases. However, the scheme structure does not depend on the term order: indeed, we define the functor of liftings of H and prove that it is represented by a scheme L_H. Our approach allows to embed L_H in a Hilbert scheme as a locally closed subscheme, with the consequence that its radical locus is an open subset. Moreover, over an infinite field, we show that every saturated ideal defining a Cohen-Macaulay scheme of codimension two has a radical x_n-lifting, giving in particular an answer to an open question posed by L. G. Roberts.

1. Introduction

Let K be a field and A be a K-algebra. We consider the lifting problem as proposed in terms of ideals first in [4] and then in [9] and, equivalently, in terms of K-algebras by Grothendieck (e.g. [9] and the references therein). Many authors have investigated this interesting problem, sometimes also describing particular lifting procedures to construct algebraic varieties with specific properties (see for instance [7] and the references therein).

Definition 1.1. Let H be a homogeneous ideal of $K[\mathbf{x}] := K[x_0, \dots, x_{n-1}]$ and A be a K-algebra. A homogeneous ideal I of $A[\mathbf{x}, x_n] := K[x_0, \dots, x_n] \otimes_K A$ is called a *lifting of H with respect to x_n* or a *x_n-lifting of H* if the following conditions are both satisfied:
(a) x_n is a non-zero divisor in $A[\mathbf{x}, x_n]/I$;
(b) $(I, x_n)/(x_n) \simeq H$, i.e., $H = (g(x_0, x_1, \dots, x_{n-1}, 0) : \forall g \in I)$.
The ideal I is a *radical lifting* of H if it is a x_n-lifting of H and it is a radical ideal.

We propose and use a new approach that is based on the theory of representable functors. Indeed, we define *the functor of liftings* $\underline{\mathrm{L}}_H$ of a homogeneous polynomial ideal H and show that it is representable, in the perspective given by [6] for Gröbner strata and according to the point of view of [1]. We can explicitly compute equations defining *the scheme of liftings* of H, i.e., the scheme L_H that parameterizes the liftings of H and represents the functor, by a reformulation of a result of [3] in terms of Gröbner bases.

The subset of L_H whose elements correspond to radical liftings of H is the *radical locus of* L_H. An almost immediate consequence of our approach is that a scheme of liftings can be embedded in a Hilbert scheme and also its radical locus is an open subset.

Moreover, we are able to prove that every saturated ideal defining a Cohen-Macaulay scheme of codimension two has a radical lifting. This result is particularly significant in the context of the study of radical liftings, because of the lack of information endured until now and highlighted in [8] in the case of polynomial homogeneous ideals in three variables.

For detailed proofs and examples, see [2].

2. Notations and main tool

Let $\mathbb{T}_{\mathbf{x}}$ and $\mathbb{T}_{\mathbf{x},x_n}$ be the set of terms in the variables $\mathbf{x} = \{x_0, \dots, x_{n-1}\}$ and $\mathbf{x} \cup \{x_n\}$, respectively. We consider the variables ordered as $x_0 > x_1 > \cdots > x_n$. All commutative rings have unit such that $1 \neq 0$ and every morphism preserves the unit.

Definition 2.1. Let $\prec$ be a term order on $\mathbb{T}_{\mathbf{x}}$. We denote by $\prec_n$ the corresponding *degreverse term order* on $\mathbb{T}_{\mathbf{x},x_n}$, which is the graded term order such that: for two terms x^α and x^β in $\mathbb{T}_{\mathbf{x},x_n}$ of the same degree, $x^\alpha \preceq_n x^\beta$ if $\alpha_n > \beta_n$ or $\alpha_n = \beta_n$ and $(x^\alpha / x_n^{\alpha_n}) \preceq (x^\beta / x_n^{\beta_n})$.

We always consider homogeneous polynomials with coefficients in the K-algebra A and homogeneous ideals given by monic Gröbner bases. This is a key point for the use of functors we introduce, because of the following two facts: firstly, there is no ambiguity when using the terminology "initial ideal", because the head terms of the polynomials in the Gröbner bases we consider have coefficient 1; secondly, monic Gröbner bases are preserved under extension of scalars [1]. The following result is a reformulation of [3, Theorem 2.5] in terms of Gröbner bases. It is the key tool of our strategy of investigation of x_n-liftings.

Theorem 2.2. *Let A be a K-algebra, H be a homogeneous ideal of $K[\mathbf{x}]$, I be a homogeneous ideal of $A[\mathbf{x}, x_n]$, $\prec$ be a term order on $K[\mathbf{x}]$ and $\prec_n$ be the corresponding degreverse term order on $A[\mathbf{x}, x_n]$. Then, the following conditions are equivalent:*

(i) the ideal I is a x_n-lifting of H;

(ii) the reduced Gröbner basis of I w.r.t. $\prec_n$ on $A[\mathbf{x}, x_n]$ is $\{f_\alpha + g_\alpha\}_\alpha$, where $\{f_\alpha\}_\alpha$ is the reduced Gröbner basis of H w.r.t. $\prec$ and, for every α, $g_\alpha \in (x_n)$ is a homogeneous polynomial in $A[\mathbf{x}, x_n]$ of degree $\deg(f_\alpha)$.

3. The functor of liftings of a homogeneous polynomial ideal

By Theorem 2.2, we can define the following functor.

Definition 3.1. Let $H \subseteq K[\mathbf{x}]$ be a homogeneous ideal. We define the *functor of liftings* of H

$$\underline{\mathrm{L_H}} : \underline{K - \mathrm{Alg}} \to \underline{\mathrm{Set}}$$

in the following way: $\underline{\mathrm{L_H}}$ associates to any K-algebra A the set $\underline{\mathrm{L_H}}(A) := \{I \subseteq A[\mathbf{x}, x_n] : I \text{ is a } x_n\text{-lifting of } H\}$ and to any morphism of K-algebras $\phi : A \to B$ the map $\underline{\mathrm{L_H}}(\phi) : \underline{\mathrm{L_H}}(A) \to \underline{\mathrm{L_H}}(B)$ such that $\underline{\mathrm{L_H}}(\phi)(I) = I \otimes_A B$.

Given the homogeneous ideal H in $K[\mathbf{x}]$ and its reduced Gröbner basis $F := \{f_\alpha\}_\alpha$ w.r.t. $\prec$, we denote by $\mathfrak{j}$ the ideal $\mathrm{in}_\prec(H)$ and by J the monomial ideal generated by $\mathfrak{j}$ in $A[\mathbf{x}, x_n]$. For every $x^\alpha \in \mathfrak{j}$ we define

$$G_\alpha := \sum_{\substack{x_n x^\gamma \notin J \\ |\gamma|+1=|\alpha|}} C_{\alpha\gamma} x_n x^\gamma, \quad \mathcal{G} = \{f_\alpha + G_\alpha\}_\alpha. \tag{1}$$

where the $C_{\alpha\gamma}$'s are new variables. We set $C := \{C_{\alpha\gamma}\}_{\alpha,\gamma}$ and we extend $\prec_n$ to any elimination term order of the variables $\mathbf{x}, x_n$ on $K[C][\mathbf{x}, x_n]$.

Theorem 3.2. *Let H, F, $\mathcal{G}$, $\prec$ and $\prec_n$ be as above and let $\mathfrak{h}$ be the smallest ideal in $K[C]$, with Gröbner basis $\mathcal{H}$, such that $\mathcal{G} \cup \mathcal{H}$ is a Gröbner basis in $K[C][\mathbf{x}, x_n]$. The affine scheme $\mathrm{L}_H := \mathrm{Spec}(K[C]/\mathfrak{h})$ represents the functor $\underline{\mathrm{L}_H}$ and we call it* the scheme of liftings of H.

We can compute a set of generators of the ideal $\mathfrak{h}$ of Theorem 3.2 by an explicit algorithmic construction, similar to the one in [6] for Gröbner strata.

Example 3.3. [2, Example 7.1] By Theorem 3.2, we compute the scheme of x_3-liftings of the lex-segment ideal $J := (x_0^2, x_0x_1, x_0x_2, x_1^2) \subseteq K[x_0, x_1, x_2]$, using the degreverse term order corresponding to the lex. We obtain that L_J is a reduced scheme with two irreducible components: L_1 isomorphic to $\mathbb{A}^7_K$ and L_2 isomorphic to $\mathbb{A}^4_K$. Further, every point of L_2 corresponds to a non-radical lifting of H.

We underline that the construction of the ideal $\mathfrak{h}$ explicitly involves the term order, nevertheless the scheme $\mathrm{Spec}(K[C]/\mathfrak{h})$ does not depend on it. Namely, if we consider two different term orders $\prec_n$ and $\prec'_n$ and construct the ideals $\mathfrak{h} \subseteq K[C]$ and $\mathfrak{h}' \subseteq K[C']$ respectively, by Yoneda's lemma $\mathrm{Spec}(K[C]/\mathfrak{h}) \simeq \mathrm{Spec}(K[C']/\mathfrak{h}')$. This isomorphism is not trivial: generally it is not induced by a linear change of variables and $|C| \neq |C'|$ [2, Example 7.2].

4. Embedding L_H in the Hilbert scheme

Let J be a monomial ideal. Let $\underline{\mathrm{St}}_J^{\prec_n}(A)$ be the set containing the homogeneous ideals $I \subseteq A[\mathbf{x}, x_n]$ having J as initial ideal with respect to $\prec_n$. The map $\underline{\mathrm{St}}_J^{\prec_n}$ between the category of K-algebras and that of sets is a representable functor and we call its representing scheme *Gröbner stratum scheme*, denoted by $\mathrm{St}_J^{\prec_n}$. For the construction of the representing scheme $\mathrm{St}_J^{\prec_n}$ and some of its main features, we refer to [6].

Proposition 4.1. *Let $J \subset A[\mathbf{x}, x_n]$ be a monomial ideal such that $\mathrm{Proj}(A[\mathbf{x}, x_n]/J)$ has Hilbert polynomial $p(t)$ and assume that $B_J \subset \mathbb{T}_{\mathbf{x}}$ and that $\prec_n$ is a degreverse term order. Then $\mathrm{St}_J^{\prec_n} \cong \mathrm{St}_{J_{\geq m}}^{\prec_n}$, for every integer m. Moreover, $\mathrm{St}_J^{\prec_n}$ can be embedded in the Hilbert scheme $\mathcal{H}\mathrm{ilb}^n_{p(t)}$ as a locally closed subscheme.*

Theorem 4.2. *In the above settings, $\underline{\mathrm{L}}_H$ is a closed subfunctor of $\underline{\mathrm{St}}_J^{\prec_n}$ and L_H is locally closed in the Hilbert scheme $\mathcal{H}\mathrm{ilb}^n_{p(t)}$. Further, the radical locus of L_H is open in L_H.*

5. Liftings of a Cohen-Macaulay scheme of codimension two

Let $H \subset K[\mathbf{x}]$ be a saturated homogeneous ideal such that $\mathrm{Proj}(K[\mathbf{x}]/H)$ is a Cohen-Macaulay scheme of codimension 2. Hence, there is a graded free resolution of type

$$0 \longrightarrow K[\mathbf{x}]^a \xrightarrow{\psi_2} K[\mathbf{x}]^{a+1} \xrightarrow{\psi_1} K[\mathbf{x}] \longrightarrow K[\mathbf{x}]/H \longrightarrow 0. \tag{2}$$

The Hilbert-Burch Theorem guarantees that the $a \times a$ minors of the $a \times (a+1)$ matrix M_H of the homomorphism ψ_2 in (2) form a set of generators for H. Further, the rows of this matrix generate the first syzygies module of H. Vice versa, a 2-codimensional scheme defined by the $a \times a$ minors of a $a \times (a+1)$ matrix is a Cohen-Macaulay scheme.

Lemma 5.1. *Let K be an infinite field, H be as above and I be a x_n-lifting of H.*

(1) Replacing x_n by 0 in a first syzygy of the Gröbner basis of I, we get a first syzygy of the Gröbner basis of H.

(2) If $\prec$ is the degrevlex term order, there is a free resolution of H (resp. I) of type (2) obtained by "lifting" a minimal free resolution of $\mathfrak{j}$ (resp. J).

Theorem 5.2. *The scheme of liftings L_H of H is an affine space $\mathbb{A}^D_K$, for a suitable D.*

Proof. By Lemma 5.1, we consider the free resolution (2) of H. We add to each entry of the matrix M_H a linear combination of the terms divisible by x_n of the appropriate degree. This new matrix gives a x_n-lifting of H. □

Example 5.3. [2, Example 7.3] We consider the saturated ideal $H = (x_0^2 - x_1^2, x_0x_1 + 2x_1^2, x_1^3)$ in $K[x_0, x_1, x_2]$, defining a zero dimensional scheme in $\mathbb{P}^2$. In this case L_H is $\mathbb{A}^{11}_K$.

Theorem 5.4. *Every saturated homogeneous ideal H defining a 2-codimensional Cohen-Macaulay scheme over an infinite field K has a radical x_n-lifting. In particular, every saturated homogeneous ideal defining a 0-dimensional scheme in $\mathbb{P}^2_K$ has a radical x_n-lifting.*

Proof. Let $\mathfrak{j}$ be the initial ideal of H w.r.t. the degrevlex term order. Let $\{H(t)\}_t$ be a flat family of Gröbner deformations from H to $\mathfrak{j}$. For $H(t)$ and $\mathfrak{j}$ there are free resolutions of type (2), because of the Cohen-Macaulay property. Let $M_{H(t)}$ and $M_{\mathfrak{j}}$ be the matrices of the morphisms ψ_2 in these resolutions. Let N be a radical x_n-lifting of $\mathfrak{j}$ (see [4]) and let M_N be the matrix of the morphism ψ_2 of a free resolution of type (2) for N. Such a resolution of N exists because a x_n-lifting of a Cohen-Macaulay ideal is Cohen-Macaulay.

We obtain a flat family $\{I(t)\}_t$ of x_n-liftings of $\{H(t)\}_t$, parameterized by the matrix $M(t) := M_{H(t)} + M_N - M_{\mathfrak{j}}$, and we can embed it in a Hilbert scheme, whose radical locus is open [5, Théorème (12.2.1)]. Let U be the open subset of $\mathbb{A}^1$ parameterizing the reduced schemes in $\{I(t)\}_t$. U is non-empty, since it contains the point $t = 0$. Since K is infinite, there is $0 \neq \bar{t} \in U$ such that $I(\bar{t})$ defines a reduced scheme. From this ideal we can obtain a radical x_n-lifting of H, by applying the automorphism of $\mathbb{P}^n$ induced by the Gröbner deformations on $I(\bar{t})$. □

References

[1] D. Bayer, A. Galligo, M. Stillman, *Gröbner bases and extension of scalars*, Computational algebraic geometry and commutative algebra (Cortona, 1991), Sympos. Math., XXXIV, 1993, pp. 198–215.

[2] C. Bertone, F. Cioffi, M. Guida, M. Roggero, *The scheme of liftings and applications*, arXiv:1312.7700 [math.AG], 2013.

[3] G. Carrà Ferro, L. Robbiano, *On super G-bases*, J. Pure Appl. Algebra **68** (1990), no. 3, 279–292.

[4] A. V. Geramita, D. Gregory, L. Roberts, *Monomial ideals and points in projective space*, J. Pure Appl. Algebra **40** (1986), no. 1, 33–62.

[5] A. Grothendieck, *Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas IV*, Inst. Hautes Études Sci. Publ. Math. (1967), no. 32, 361.

[6] P. Lella, M. Roggero, *On the functoriality of marked families*, arXiv:1307.7657 [math.AG], 2013.

[7] T. Luo, E. Yilmaz, *On the lifting problem for homogeneous ideals*, J. Pure Appl. Algebra **162** (2001), no. 2-3, 327–335.

[8] L. G. Roberts, *On the lifting problem over an algebraically closed field*, C. R. Math. Rep. Acad. Sci. Canada **11** (1989), no. 1, 35–38.

[9] M. Roitman, *On the lifting problem for homogeneous ideals in polynomial rings*, J. Pure Appl. Algebra **51** (1988), no. 1-2, 205–215.

Bertone, Roggero: Dip. di Matematica dell'Università di Torino, Italy
E-mail address: cristina.bertone@unito.it, margherita.roggero@unito.it

Cioffi, Guida: Dip. di Matematica e Applicazioni dell'Università di Napoli "Federico II", Italy
E-mail address: cioffifr@unina.it, maguida@unina.it

AN ALGORITHM FOR PRODUCING F-PURE IDEALS

ALBERTO F. BOIX AND MORDECHAI KATZMAN

ABSTRACT. This report describes a method for computing all F-pure ideals for a given p^{-1}-linear map of a polynomial ring over a finite field.

INTRODUCTION

The subject of this report is the study of certain ideals associated with a given p^{-e}*-linear map*; these maps were introduced by K. Schwede in [6] and M. Blickle in [1] in the context of test ideals.

Hereafter, we shall denote by S the polynomial ring $\mathbb{Z}/p\mathbb{Z}[x_1, \dots, x_d]$, where p is a prime number, and $\mathfrak{m}$ will stand for the ideal of S generated by all the variables.

These p^{-e}-linear maps referred to above are additive maps $S \xrightarrow{\phi_e} S$ such that $\phi(s^{p^e} t) = s\phi(t)$ for all $s, t \in S$; in this way, if we denote by $\operatorname{End}_{p^{-e}}(S)$ the set of all p^{-e}-linear maps, then we can pack them as follows:

$$\mathcal{C}^S := \bigoplus_{e \geq 0} \operatorname{End}_{p^{-e}}(S).$$

Since the composition of a p^{-e}-linear map followed by a $p^{-e'}$-linear map produces a $p^{-(e+e')}$-linear map, $\mathcal{C}^S$ can be regarded as a graded S-algebra; keeping this in mind, we set

$$\mathcal{C}^S_+ := \bigoplus_{e \geq 1} \operatorname{End}_{p^{-e}}(S)$$

as the irrelevant ideal of $\mathcal{C}^S$.

In this report, we shall be mostly interested in certain graded subalgebras of $\mathcal{C}^S$; taking this into account, we introduce the objects of our study.

Definition. Let $\mathcal{C}$ be a graded S-subalgebra of $\mathcal{C}^S$. An ideal I of S is called F*-pure* (with respect to $\mathcal{C}$) provided $\mathcal{C}_+ I = I$.

Our purpose is to introduce an effective method in order to calculate all the F-pure ideals of S contained in $\mathfrak{m}$ with respect to the subalgebra of $\mathcal{C}^S$ generated by a single p^{-e}-linear map ϕ. This procedure has been implemented in Macaulay2; full details of this algorithm worked out in greater generality can be found in [3].

This work is motivated by the study of F-pure ideals and their properties carried out by M. Blickle in [1]; for instance, under our assumptions one has that S itself is an F-pure ideal (with respect to $\mathcal{C}^S$) if and only if $\mathcal{C}^S_+$ contains a splitting of a certain power of the Frobenius map on S (cf. [1, Proposition 3.5]); therefore, these F-pure ideals turn out to be a generalization of the F-purity property.

Furthermore, among the main results obtained in [1] (see also [2, Corollary 4.20 and Proposition 5.4]) is the fact that the set of F-pure ideals in S is finite, and that the big test ideal is the minimal element of such set. Apart from their usefulness in describing big test ideals, we believe that the set of F-pure ideals provides an interesting set of invariants of S yielding information about the ring which is not yet fully understood.

The reader should contrast this with the situation one encounters when studying the set of $\mathcal{C}_+^S$-compatible ideals; that is, ideals $I \subseteq S$ for which $\mathcal{C}_+^S I \subseteq I$. One might hope to list all F-pure ideals by listing all compatible ideals and checking which ones are F-pure. However, the set of compatible ideals need not be finite, and one can only describe algorithmically the radical ideals among these; such task was carried out in [5].

Our contribution to the understanding of F-pure ideals is to provide an effective procedure to calculate all the F-pure ideals contained in $\mathfrak{m}$ of the subalgebra $\mathcal{C} = \mathcal{C}^\phi$ of $\mathcal{C}^S$ generated by a single p^{-e}-linear map ϕ.

1. Compatible and fixed ideals

In what follows, ϕ will always denote a fixed p^{-e}-linear map; thus, if $\mathcal{C}$ is the subalgebra of $\mathcal{C}^S$ generated by such a ϕ, then the problem of finding the F-pure ideals of S with respect to $\mathcal{C}$ amounts to finding all ideals $I \subseteq S$ such that $\phi(I) = I$. This fact leads us to introduce the following:

Definition 1.1. It is said that an ideal I of S is *ϕ-compatible* (respectively, *ϕ-fixed*) if $\phi(I) \subseteq I$ (respectively, $\phi(I) = I$).

On the other hand, it is known (cf. [4, Example 1.3.1]) that any p^{-e}-linear map ϕ can be written as $\pi_e \circ u$ for some $u \in S$, where $S \xrightarrow{\pi_e} S$ is the unique p^{-e}-linear map which is the projection onto the direct summand $Sx_1^{p^e-1} \cdots x_d^{p^e-1}$.

Our next goal is to express in an equivalent way the condition of being ϕ-fixed in order to carry out explicit computations. Such equivalent expression requires us to introduce the following concept.

Definition 1.2. Let J be an ideal of S. We set $I_e(J)$ as the smallest ideal (namely, I) such that $I^{[p^e]} \supseteq J$.

This notion, combined with the fact that $\phi = \pi_e \circ u$, allows us to express the condition of being ϕ-fixed in computational terms, as described in the next result, whose proof is omitted (cf. [3, Theorem 1.4]).

Lemma 1.3. *An ideal J of S is ϕ-compatible (respectively, fixed) if and only if $I_e(uJ) \subseteq J$ (respectively, $I_e(uJ) = J$).*

It is worth noting that the ideal $I_e(J)$ is highly computable; the interested reader may like to consult [5, pp. 1003–1004] for further details.

2. The algorithm through the hash operation

Before going on, we fix some additional notation. Given $\alpha = (a_1, \dots, a_d) \in \mathbb{N}^d$, we shall use the following multi-index notation:

$$\mathbf{x}^\alpha := x_1^{a_1} \cdots x_d^{a_d}.$$

Moreover, in this case, we set $||\mathbf{x}^\alpha|| := \max\{a_1, \dots, a_d\}$ and, for any $g \in S$,

$$||g|| := \max_{\alpha \in \operatorname{supp}(g)} ||\mathbf{x}^\alpha||,$$

where $g = \sum_{\alpha \in \mathbb{N}^d} g_\alpha \mathbf{x}^\alpha$ (such that $g_\alpha = 0$ up to a finite number of terms) and

$$\operatorname{supp}(g) := \left\{ \alpha \in \mathbb{N}^d \mid \quad g_\alpha \neq 0 \right\}.$$

The aim of this section is to describe a computational method in order to produce all the ϕ-fixed ideals of S. As the reader will appreciate, our procedure is based on a new operation on ideals which we hope to be of some interest in its own right. Such operation is described in the next:

Definition 2.1. Let J be any ideal of S, set

$$D_e := \left\lceil \frac{||u||}{p^e - 1} \right\rceil,$$

and S_{D_e} to be the $\mathbb{Z}/p\mathbb{Z}$-vector space generated by monomials $\mathbf{x}^\alpha$ with $||\alpha|| \leq D_e$. We define the sequence of ideals

$$J_0 := J, \quad J_{i+1} := \left(J_i \cap (J_i^{[p^e]} :_S u) \cap I_e(uJ_i) \cap S_{D_e} \right) S,$$

and set

$$J^{\#_e} := \bigcap_{i \geq 0} J_i.$$

When $e = 1$, we write $J^{\#}$ rather than $J^{\#_1}$; we refer to this construction as the *hash operation*.

The introduction of the hash operation is motivated by the following result; we omit its proof and refer to [3, Lemma 2.3] for details.

Lemma 2.2. *For any ideal J of S, $J^{\#_e}$ contains all the ϕ-fixed ideals which are contained in J.*

The following algorithm is the main result of this report.

Algorithm 2.3. The input data are: a prime number p, $S = \mathbb{Z}/p\mathbb{Z}[x_1, \dots, x_d]$ and $u \in S$. We initialize $I = S$ and L as the empty list. From now on, execute the following commands:

(i) Compute $I^{\#_e}$. Assign to I the value of $I^{\#_e}$.
(ii) If $I_e(uI) = I$, then add I to the list L.
(iii) If $I = 0$, then stop and output the list L.
(iv) If $I \neq 0$ but principal, assign to I the value of $\mathfrak{m}I$ and loop over the previous steps.
(v) If $I \neq 0$ and not principal, then compute

$$\left\{ V \quad \text{ideal} \mid \quad \mathfrak{m}I \subseteq V \subseteq I, \quad \dim_{\mathbb{Z}/p\mathbb{Z}} I/V = 1 \right\}.$$

For each element V of such set, loop over the previous steps.

The output is the list L of all the ϕ-fixed ideals of S contained in $\mathfrak{m}$, where $\phi = \pi_e \circ u$.

Sketch of proof of correctness. First of all, lemma 2.2 justifies steps (i), (ii), and (iii). Secondly, step (iv) is essentially due to the fact that we are only interested in the fixed ideals contained in $\mathfrak{m}$. Finally, step (v) guarantee (slightly loosely speaking) that we do not forget fixed ideals by the way. Therefore, this procedure is recursive and one should justify the finiteness of the resulting execution tree; however, such finiteness holds because the chains of $V^{\#_e}$'s produced in this recursion have length at most $\dim_{\mathbb{Z}/p\mathbb{Z}} S_{D_e}$. The reader is referred to [3, Theorem 2.4] for additional details. □

3. An example

We finish this report by exhibiting an example where we develop our method step by step for the convenience of the reader.

Example 3.1. We consider the ring $S := \mathbb{Z}/2\mathbb{Z}[x, y]$ and set $u := xy$. We compute L, the list of ϕ-fixed ideals of S, where $\phi = \pi_1 \circ u$.

Start with $I = S = I^{\#}$. As $I_1(uI) = I$ add S to the list L. Next, since I is principal, go on with $I = \mathfrak{m} = I^{\#}$; as $I_1(uI) = I$ add $\mathfrak{m}$ to the list L. Moreover, we have to note that

$$\left\{\mathfrak{m}^2 \subseteq V \subseteq \mathfrak{m} \mid \quad \dim_{\mathbb{Z}/2\mathbb{Z}} \mathfrak{m}/V = 1\right\} = \left\{\langle x, y^2\rangle, \langle y, x^2\rangle, \langle x^2, xy, x + y\rangle\right\}.$$

We have to stress that in the calculation of this set is when we are using that we are working with characteristic two.

Now, since $\langle x^2, xy, x + y\rangle^{\#} = \langle xy\rangle$ and $I_1(u\langle xy\rangle) = \langle xy\rangle$ add $\langle xy\rangle$ to the list L. Moreover, as $\langle xy\rangle$ is principal go on with $\langle x^2y, xy^2\rangle$. Nevertheless, since $\langle x^2y, xy^2\rangle^{\#} = \langle 0\rangle$ we stop this branch of the recursion tree. On the other hand, since $\langle x, y^2\rangle^{\#} = \langle x\rangle$ and $I_1(u\langle x\rangle) = \langle x\rangle$ add $\langle x\rangle$ to the list L. In addition, as $\langle x\rangle$ is principal go on with $\langle x^2, xy\rangle$. However, since $\langle x^2, xy\rangle^{\#} = \langle xy\rangle$ we can use the foregoing calculations and therefore we can conclude that this branch of the recursion tree produces no new fixed ideals. A similar computation shows that we only have to add $\langle y\rangle$ to L.

In this way, it follows that $L = \{\mathbb{Z}/2\mathbb{Z}[x, y], \langle x, y\rangle, \langle x\rangle, \langle y\rangle, \langle xy\rangle, \langle 0\rangle\}$.

References

[1] M. Blickle. Test ideals via algebras of p^{-e}-linear maps. *J. Algebraic Geom.*, 22(1):49–83, 2013.

[2] M. Blickle and G. Böckle. Cartier modules: finiteness results. *J. Reine Angew. Math.*, 661:85–123, 2011.

[3] A. F. Boix and M. Katzman. An algorithm for producing F-pure ideals. Available at http://arxiv.org/pdf/1307.6717v1, 2013.

[4] M. Brion and S. Kumar. *Frobenius splitting methods in geometry and representation theory*, volume 231 of *Progress in Mathematics*. Birkhäuser Boston Inc., Boston, MA, 2005.

[5] M. Katzman and K. Schwede. An algorithm for computing compatibly Frobenius split subvarieties. *J. Symbolic Comput.*, 47(8):996–1008, 2012.

[6] K. Schwede. Test ideals in non-$\mathbb{Q}$-Gorenstein rings. *Trans. Amer. Math. Soc.*, 363(11):5925–5941, 2011.

Department of Economics and Business, Universitat Pompeu Fabra, Jaume I Building, Ramon Trias Fargas 25-27, 08005 Barcelona, Spain.

E-mail address: alberto.fernandezb@upf.edu

Department of Pure Mathematics, University of Sheffield, Hicks Building, Sheffield S3 7RH, United Kingdom

E-mail address: M.Katzman@sheffield.ac.uk

REDUCTION OF ROESSER'S 2-D LINEAR DISCRETE SYSTEMS USING SYMBOLIC COMPUTATION

MOHAMED S. BOUDELLIOUA

ABSTRACT. In this paper, symbolic computation is used to obtain a canonical form for polynomial matrices arising from discrete 2-D linear state-space Roesser systems. The canonical form which can be regarded as an extension of the companion form often encountered in the theory of 1-D linear systems. Using previous results obtained by Boudellioua and Quadrat [4] on the reduction by equivalence to Smith form, the exact transformation connecting the original polynomial matrix and the reduced canonical form is set out. In this paper, using symbolic computation based on the OREMODULES [5] Maple package the connection between the original polynomial matrix and the canonical form is established.

INTRODUCTION

A 2-D system is a system in which information propagates in two independent directions. These systems arise from applications such as image processing, iterative circuits, etc. Several authors (Attasi [1], Fornasini-Marchesini [6] and Roesser [9]) have proposed different state-space models for 2-D discrete linear systems. However, it has been shown that Roesser's model is the most satisfactory and the most general since the other models can be embedded in it. The model of Roesser is one in which the local state is divided into horizontal and a vertical state which are propagated respectively horizontally and vertically by first order difference equations. The model has the form:

$$\begin{aligned} x^h(i+1,j) = &\quad A_1x^h(i,j) + A_2x^v(i,j) + B_1u(i,j) \\ x^v(i,j+1) = &\quad A_3x^h(i,j) + A_4x^v(i,j) + B_2u(i,j) \end{aligned} \tag{1}$$

where $x^h(i,j)$ is the horizontal state vector, $x^v(i,j)$ is the vertical state vector, $u(i,j)$ is the input vector, and $A_1, A_2, A_3, A_4, B_1, B_2$, are real constant matrices of appropriate dimensions. The system (1) can be written in the polynomial form:

$$\begin{pmatrix} sI_n - A_1 & -A_2 \\ -A_3 & zI_m - A_4 \end{pmatrix} \begin{pmatrix} x^h(i,j) \\ x^v(i,j) \end{pmatrix} = \begin{pmatrix} B_1 \\ B_2 \end{pmatrix} u(i,j) \tag{2}$$

where s represents an advance operator in the horizontal direction and z an advance operator in the vertical direction. The polynomial matrix over $\mathbb{R}[s,z]$,

$$T(s,z) = \begin{pmatrix} sI_n - A_1 & -A_2 \\ -A_3 & zI_m - A_4 \end{pmatrix} \tag{3}$$

is the characteristic matrix associated with (1). Throughout this paper unless specified otherwise, $D = K[z_1, \ldots, x_n]$, denotes the polynomial ring in the indeterminates $x_1, \ldots, x_n$ with coefficients in an arbitrary but fixed field K.

Theorem 0.1 ([7, 8, 4])**.** *Let $T \in D^{p\times p}$, with full row rank, then T is unimodular equivalent to the Smith form*

$$S = \begin{pmatrix} I_{p-1} & 0 \\ 0 & |T| \end{pmatrix} \tag{4}$$

where $|T| \equiv \det(T) \in D$ if and only if there exist a vector $U \in D^p$ which admits a left inverse over D such that the matrix $\begin{pmatrix} T & U \end{pmatrix}$ has a right inverse over D.

1. Canonical Form for 2-D Roesser Matrices

Canonical forms play an important role in the theory of linear systems. Many of the concepts that lie at the centre of systems theory such as controllability, observability and stability can be linked via companion form matrices, see for example Barnett [2]. In the following a generalization of a canonical form 1-D to the 2-D setting is presented for systems arising from Roesser's discrete state-space models. The canonical form is based on companion form matrices and is such that many of the properties are readily extended from 1-D to the 2-D.

Let $D = \mathbb{R}[s, z]$ and introduce the canonical form $T_F \in D^{(n+m)\times(n+m)}$ given in [3] for a matrix T in the form (3):

$$T_F = \begin{pmatrix} sI_n - F_1 & -\bar{A}_2 \\ -\bar{A}_3 & zI_m - F_4 \end{pmatrix} \tag{5}$$

where F_1 and F_2 are in companion form, i.e.,

$$F_1 = \begin{pmatrix} 0 & 1 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ -\alpha_n & -\alpha_{n-1} & \cdots & -\alpha_1 \end{pmatrix}, \quad F_4 = \begin{pmatrix} 0 & 1 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ -\beta_m & -\beta_{m-1} & \cdots & -\beta_1 \end{pmatrix}, \tag{6}$$

$\bar{A}_2 = \begin{pmatrix} E_n & 0 \end{pmatrix}$ and E_n is the n-th column of I_n. Setting $|T| = |T_F|$, determines uniquely the matrix $\bar{A}_3 = [a_{ij}]$. The canonical form in (5) has the property that $\begin{pmatrix} T_F & E_{n+m} \end{pmatrix}$ admits a right inverse over D leading to the establishment of the following lemma.

Lemma 1.1. *The matrix in the canonical form T_F in (5) is unimodular equivalent to the Smith form (4).*

The following result is a consequence of Theorem 0.1 and Lemma 1.1.

Theorem 1.2. *Let T be a polynomial matrix in the form (3) satisfying the condition given in Theorem 0.1, then T is unimodular equivalent over D to the canonical form T_F in (5).*

2. Computational Aspects

Example 2.1. Let $D = \mathbb{R}[s, z]$ and

$$T = \left(\begin{array}{cc|cc} s+1 & -1 & -1 & 1 \\ 1 & s & -1 & 1 \\ \hline 2 & -2 & z+1 & -3 \\ 0 & -3 & 2 & z-2 \end{array}\right)$$

where $|T| = (s^2+s+1)z^2 + (-s^2+2s+1)z + 4s^2 - 2s + 4$. The matrix in canonical form T_F associated with $|T|$ is given by (see [3]) :

$$T_F \equiv \begin{pmatrix} sI_2 - F_1 & -\bar{A}_2 \\ -\bar{A}_3 & zI_2 - F_4 \end{pmatrix} = \left(\begin{array}{cc|cc} s & -1 & 0 & 0 \\ 1 & s+1 & -1 & 0 \\ \hline 2 & 3 & z & -1 \\ 2 & -3 & 4 & z-1 \end{array}\right) \tag{7}$$

First we reduce the matrix T to the Smith form S, i.e., compute $M_1 \in GL_4(D)$ and $N_1 \in GL_4(D)$ such that $S = M_1 T N_1$ where S is given by (4). Using the method given by Boudellioua and Quadrat [4], consider the vector $U_1 = \begin{pmatrix} 0 & 0 & -1 & -1 \end{pmatrix}^T \in D^4$ and $P_1 = (T \quad U_1) \in D^{4\times 5}$. Using the package OREMODULES in Maple, see Chyzak *et al.* [5], it is possible to check that P admits a right inverse over D. Furthermore, using the same package, a minimal parametrization $Q_m \in D^5$ of P, where $Q_m = (Q_1^T \quad Q_2^T)^T$ and $P_1 Q_m = 0$, is computed

$$Q_m = \begin{pmatrix} Q_1 \\ Q_2 \end{pmatrix} = \left(\begin{array}{c} 2s+2 \\ 2s \\ (z+1)s^2 + (z+4)s + z + 3 \\ (z-1)s^2 + (z+2)s + z + 1 \\ \hline (z^2 - z + 4)s^2 + (z^2 + 2z - 2)s + z^2 + z + 4 \end{array}\right) \tag{8}$$

Computing the SyzygyModule $K_1 \in D^{3\times 4}$ of Q_1, i.e., $K_1 Q_1 = 0$ gives

$$K_1 = \begin{pmatrix} 2 & 1 & z-1 & -z-1 \\ 1 & s & -1 & 1 \\ s+1 & -1 & -1 & 1 \end{pmatrix} \tag{9}$$

where the matrix $Q_3 \in D^{4\times 3}$ is the right inverse of K_1, i.e.,

$$Q_3 = \begin{pmatrix} 0 & 1 & -1 \\ 0 & 1 & -1 \\ -\frac{1}{2} & \frac{3}{2} + \left(\frac{1}{2} + \frac{1}{2}z\right)s & \left(-\frac{1}{2} - \frac{1}{2}z\right)s - 2 - \frac{1}{2}z \\ -\frac{1}{2} & \frac{3}{2} + \left(-\frac{1}{2} + \frac{1}{2}z\right)s & \left(\frac{1}{2} - \frac{1}{2}z\right)s - 1 - \frac{1}{2}z \end{pmatrix} \tag{10}$$

Thus the matrix $N_1 = (Q_3 \quad Q_1) \in GL_4(D)$ is given by:

$$N_1 = \begin{pmatrix} 0 & 1 & -1 & 2+2s \\ 0 & 1 & -1 & 2s \\ -\frac{1}{2} & \frac{3}{2} + \left(\frac{1}{2} + \frac{1}{2}z\right)s & \left(-\frac{1}{2} - \frac{1}{2}z\right)s - 2 - \frac{1}{2}z & (z+1)s^2 + (4+z)s + z + 3 \\ -\frac{1}{2} & \frac{3}{2} + \left(-\frac{1}{2} + \frac{1}{2}z\right)s & \left(\frac{1}{2} - \frac{1}{2}z\right)s - 1 - \frac{1}{2}z & (z-1)s^2 + (z+2)s + z + 1 \end{pmatrix} \tag{11}$$

The matrix $M_1 = (TQ_3 \quad -U)^{-1} \in GL_4(D)$ is given by

$$M_1 = \begin{pmatrix} 0 & 0 & 1 & -1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ \left(2 - \frac{1}{2}z + \frac{1}{2}z^2\right)s + \frac{1}{2}z^2 - 1 + z & \left(-2 + \frac{1}{2}z - \frac{1}{2}z^2\right)s + 3 - \frac{3}{2}z & \frac{1}{2}z & -\frac{1}{2}z + 1 \end{pmatrix} \tag{12}$$

and it can be verified the matrix M_1TN_1 yields the Smith form

$$S = \begin{pmatrix} I_3 & 0 \\ 0 & Q_2 \end{pmatrix} \equiv \begin{pmatrix} I_3 & 0 \\ 0 & \left(s^2+s+1\right)z^2 + \left(2\,s - s^2 + 1\right)z + 4\,s^2 - 2\,s + 4 \end{pmatrix} \tag{13}$$

where $Q_2 = |T|$. Similarly, the matrix T_F is reduced to the Smith form S. Computing $M_2 \in GL_4(D)$ and $N_2 \in GL_4(D)$ such that $S = M_2T_FN_2$ where S is given by (4) yields,

$$N_2 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & s \\ 0 & -1 & -s-1 & s^2+s+1 \\ -1 & -z & -3-z-sz & s^2z+(3+z)\,s+2+z \end{pmatrix} \tag{14}$$

and

$$M_2 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ z^2+2\,z-2+\left(z^2-z+4\right)s & z^2-z+4 & -1+z & 1 \end{pmatrix} \tag{15}$$

It follows that the matrix T_F is related to the matrix T by:

$$T_F = MTN \tag{16}$$

where $M = M_2^{-1}M_1 \in GL_4(D)$ and $N = N_1N_2^{-1} \in GL_4(D)$.

3. Conclusions

In this paper, we have shown that symbolic computation in Maple can be used effectively to compute the equivalence transformations that reduce a class of 2-D Roesser matrices to a canonical form. The classes of matrices considered are those arising from 2-D Roesser systems amenable to be simplified to a single equation in one unknown.

References

[1] S. Attasi. Systèmes linéaires à deux indices. Technical Report 31, IRIA, France, 1973.

[2] S. Barnett. A matrix circle in linear control theory. *I.M.A. Bulletin*, 12:173–176, 1976.

[3] M.S. Boudellioua. A canonical matrix representation of 2-D linear discrete systems. *Journal for Engineering Sciences*, 11(2):81–90, 1999.

[4] M.S. Boudellioua and A. Quadrat. Serre's reduction of linear functional systems. *Mathematics in Computer Science*, 4(2):289–312, 2010.

[5] F. Chyzak, A. Quadrat, and D. Robertz. OreModules: A symbolic package for the study of multidimensional linear systems. In J. Chiasson and J.-J. Loiseau, editors, *Applications of Time-Delay Systems*, LNCIS 352, pages 233–264. Springer, 2007, `http://wwwb.math.rwth-aachen.de/OreModules/`.

[6] E. Fornasini and G. Marchesini. State space realization theory of two-dimensional filters. *IEEE Trans. Autom. Control*, AC-21(4):484–492, 1976.

[7] M.G. Frost and M.S. Boudellioua. Some further results concerning matrices with elements in a polynomial ring. *Int. J. Control*, 43(5):1543–1555, 1986.

[8] Z. Lin, M.S. Boudellioua, and L. Xu. On the equivalence and factorization of multivariate polynomial matrices. In *Proceedings of the 2006 international symposium of circuits and systems*, Island of Kos (Greece), 2006.

[9] R.P. Roesser. A discrete state-space model for linear image processing. *IEEE Trans. Autom. Control*, AC-20(1):1–10, 1975.

Department of Mathematics and Statistics, Sultan Qaboos University, PO Box 36, Al-Khodh, 123, Muscat, Oman.

E-mail address: `boudell@squ.edu.om`

COMPLETE INTERSECTION FOR PHYLOGENETIC GROUP-BASED MODELS

MARTA CASANELLAS, JESÚS FERNÁNDEZ-SÁNCHEZ, AND MATEUSZ MICHAŁEK

ABSTRACT. We address the problem of describing a complete intersection for the phylogenetic algebraic varieties arising from group-based models. This is carried out by explicitly constructing a system of equations that define the variety in an open set containing the points with biological sense. At the same time, our results provide an affirmative answer to a conjecture by the third author, and give some insight to a couple of conjectures by Sturmfels and Sullivant in [16].

INTRODUCTION

In model-based phylogenetics, evolution is usually modeled assumed to proceed along a tree, from a an ancestral DNA sequence located at the root of the tree, to sequences found in the taxa (which label the leaves of the tree). The bases A, C, G and T corresponding to the nucleotides are viewed as the states of random variables at the nodes of the tree, while the model rules the parameters of the probabilistic process associated with the edges of the tree. If we obtain a collection of biological sequences, from currently extant species (taxa), these sequences can be considered to have evolved from a common ancestral sequence, and be arranged in a alignment. Moreover, each site in the sequence might be assumed to evolve independently and with identical distribution, so that different sites are regarded as trial of the same probabilistic process. The main problem is then to *infer the (phylogenetic) tree* that describes the evolutionary descent of the sequences.

Phylogenetic models and trees result in algebraic varieties and motivate interesting problems in algebraic geometry, giving rise to a new area of research known as *phylogenetic algebraic geometry* [9]. Cavender and Felsenstein [6] and Lake [11], in their parallel work in 1987, were the first to propose the use of algebraic tools to deal with this problem, and since then, it has atracted much attention from algebraic geometers, specially in recent years. They were the first to introduce phylogenetic invariants for a particular model and tree, which are polynomials that vanish on all joint distributions of bases at the leaves of the tree, regardless of the values of the parameters of the model.

For applications, one might hope that the near-vanishing of phylogenetic invariants on observed frequencies of bases in DNA could be used as a test of model-fit and/or tree-topology. Therefore, it seems important to know the ideal of polynomials defining these varieties. The first approaches in this direction are due to the work of Allman-Rhodes [2] and Pachter-Sturmfels [15]. But many other authors have contributed to the development of this area, either form the more geometric point of view trying to determine minimal system of generators for the ideal of the varieties [9, 16, 1, 8, 14, 5] or from the applied standing point trying to apply them to design new methods for phylogenetic reconstruction [10, 3].

1. Minimal systems of generators for the phylogenetic ideals

Constructing a minimal system of generators of the ideal of phylogenetic invariants is a hard problem, which remains open in most cases (for example, for the most general Markov model). Besides the theoretical difficulties, the codimension of these varieties grows exponentially with the number of leaves of the tree, and the cardinal of minimal systems of generators increases even more than exponentially. Some progress has been made for models that can be described in terms of the action of a finite abelian group (Jukes-Cantor, binary Jukes-Cantor, and the Kimura models with 2 or 3 parameters). For them, one can consider new systems of parameters (Fourier parameters) to describe the corresponding varieties as toric varieties, simplifying the problem of obtain full systems of generators for the ideal. This is carried out in [16] and extended in [12].

Moreover, Sturmfels and Sullivant observe that the degree of generation for the ideal of these varieties seems to be upper bounded by the cardinality of the group, and they conjecture that for any abelian group G and any tree T, the ideal $I(X)$ of the associated phylogenetic variety is generated in degree at most $|G|$. This conjecture is open, apart from the case $G = \mathbb{Z}_2$ [16, 7] and the Kimura 3-parameter model corresponding to the group $\mathbb{Z}_2 \times \mathbb{Z}_2$ [14].

2. Complete intersections for the varieties of group-based models

A complete system of generators might have no biological interest, because the set of probability distributions forms only a (real, semialgebraic) subset of the phylogenetic variety. Generalizing some ideas of [4], in this work we propose a different approach: given a phylogenetic variety X, we construct a system of $codimX$ phylogenetic invariants that are sufficient to define X on a Zariski open set containing the biological relevant points. We do this for certain phylogenetic varieties defined via the action of a finite abelian group G. These varieties turn out to be toric and comprise the phylogenetic varieties of two well known models in biology: Kimura 3-parameter model when $G = \mathbb{Z}_2 \times \mathbb{Z}_2$, and the Felsenstein-Neyman model when $G = \mathbb{Z}_2$. We give an explicit construction of phylogenetic invariants that define the variety X on U for *any* finite abelian group G and *any* tree. This construction produces polynomials of degree at most $|G|$, providing insights to the above conjecture by Sturmfels and Sullivant.

Our main result is the following:

Theorem 2.1. *For any abelian group $G = \mathbb{Z}_{a_1} \times \cdots \times \mathbb{Z}_{a_k}$ and any tree T the associated (toric) variety X in the Zariski open set U_X given by the orbit of the torus action is a complete intersection of explicitly constructed phylogenetic invariants of degree at most* $\max(3, a_i)$.

Sketch of the proof. The proof of the theorem has several steps, and starts from cyclic groups and the tripod (the tree with 3 leaves and only one interior node) to inductively extend to arbitrary abelian groups and trees. In any case, the toricness of the varieties play a fundamental role. For the tripod, explicit generators of degree $\leq |G|$ for U_X are provided by translating equations for X into the language of matrices, and finding a minimal system for the appropriate matrix group. In the first stage this is carried out for cyclic groups and then, generalized to any abelian group. Then, the case of any trivalent tree is achieved by joining two smaller trees whose equations are already known. Finally, we deal with case of tree with any valency.

At the same time, the result gives an affirmative answer to a conjecture stated by the third author in [13]: on the orbit U_X the variety associated to a claw tree is an intersection of varieties associated to trees with nodes of strictly smaller valency.

REFERENCES

[1] ES Allman and JA Rhodes. Phylogenetic ideals and varieties for the general Markov model. *Advances in Applied Mathematics*, 40(2):127–148, 2008.

[2] ES Allman and JA Rhodes. Phylogenetic invariants for the general Markov model of sequence mutation. *Mathematical Biosciences*, 186(2):113–144, 2003.

[3] M Casanellas and J Fernández-Sánchez. Performance of a new invariants method on homogeneous and nonhomogeneous quartet trees. *Mol. Biol. Evol.*, 24(1):288–293, 2007.

[4] M Casanellas and J Fernández-Sánchez. Geometry of the Kimura 3-parameter model. *Advances in Applied Mathematics*, 41:265–292, 2008.

[5] M Casanellas and J Fernández-Sánchez. Relevant phylogenetic invariants of evolutionary models. *Journal de Mathématiques Pures et Appliquées*, 96:207–229, 2011.

[6] J Cavender and J Felsenstein. Invariants of phylogenies: A simple case with discrete states. *J. Classif.*, 4:57–71, 1987.

[7] J Chifman and S Petrović. Toric ideals of phylogenetic invariants for the general group-based model on claw trees $k_{1,n}$. *Proceedings of the 2nd international conference on Algebraic biology*, pages 307–321, 2007.

[8] J Draisma and J Kuttler. On the ideals of equivariant tree models. *Mathematische Annalen*, 344(3):619–644, 2009.

[9] N Eriksson, K Ranestad, B Sturmfels and S Sullivant. Phylogenetic algebraic geometry. *Projective Varieties with Unexpected Properties; Siena, Italy*, pages 237–256, 2004.

[10] SN Evans and TP Speed. Invariants of some probability models used in phylogenetic inference. *Ann. Statist.*, 21(1):355–377, 1993.

[11] J Lake. A rate-independent technique for analysis of nucleaic acid sequences: Evolutionary parsimony. *Mol. Biol. Evol.*, 4:167–191, 1987.

[12] M Michałek. Geometry of phylogenetic group-based models. *Journal of Algebra*, 339(1):339–356, 2011.

[13] M Michałek. Toric varieties: phylogenetics and derived categories. *PhD thesis*, 2012.

[14] M Michałek. Toric geometry of the 3-Kimura model for any tree. *Advances in Geometry*, 14(1):11–30, 2014.

[15] L Pachter and B Sturmfels. Tropical geometry of statistical models. *Proceedings of the National Academy of Sciences*, 101:16132–16137, 2004.

[16] B Sturmfels and S Sullivant. Toric ideals of phylogenetic invariants. *J. Comput. Biology*, 12:204–228, 2005.

Universitat Politècnica de Catalunya, Dept. de Matemàtica Aplicada I, Av. Diagonal 647 08028 Barcelona, Spain
E-mail address: marta.casanellas@upc.edu

Universitat Politècnica de Catalunya, Dept. de Matemàtica Aplicada I, Av. Diagonal 647 08028 Barcelona, Spain
E-mail address: jesus.fernandez.sanchez@upc.edu

Polish Academy of Sciences, ul.Śniadeckich 8, 00956 Warsaw, Poland
E-mail address: mateusz.michalek@ujf-grenoble.fr

A NOTE ON THE REPRESENTATION OF SOLVABLE LIE ALGEBRAS

MANUEL CEBALLOS, JUAN NÚÑEZ, AND ÁNGEL F. TENORIO

ABSTRACT. Every finite-dimensional complex solvable Lie algebra can be represented as a matrix Lie algebra, with upper-triangular square matrices as elements. Nevertheless, the minimal order of these matrices is unknown in general. In this paper, we draft a method to compute both that minimal order and a matrix representation of such an order for a given solvable Lie algebra. As application of this procedure, we compute minimal faithful matrix representations for several families of Lie algebras with arbitrary dimensions.

INTRODUCTION

In virtue of Ado's Theorem, every finite-dimensional complex Lie algebra is isomorphic to a Lie subalgebra of the general linear algebra $\mathfrak{gl}(n;\mathbb{C})$ of complex $n \times n$ matrices, for some $n \in \mathbb{N}$. This paper deals with finding Lie subalgebras of Lie algebra $\mathfrak{h}_n$, of $n \times n$ upper-triangular matrices, being isomorphic to solvable Lie algebras; since every finite-dimensional solvable Lie algebra is isomorphic to a subalgebra of $\mathfrak{h}_n$, for some $n \in \mathbb{N}$, according to [7, Proposition 3.7.3]. Consequently, it is interesting to determine which is the minimal $n \in \mathbb{N}$ such that a given Lie algebra $\mathfrak{g}$ is isomorphic to some Lie subalgebra of $\mathfrak{h}_n$; i.e. finding out the minimal dimension of faithful representations of $\mathfrak{g}$ by using $n \times n$ upper-triangular matrices.

This topic has been previously studied in the literature. For example, Benjumea et al. [1] designed an algorithmic procedure which computed the minimal faithful unitriangular matrix representations of nilpotent Lie algebras. The complete list of these representations were given by Benjumea et al. [2] for nilpotent Lie algebras of dimension less than 6. With respect to filiform Lie algebras, their representations were studied in [4] for dimension less than 9. Our main goal is to obtain tools which ease the advance for the above-mentioned research and, in this way, we introduce the design of an algorithm (which has been implemented) to compute minimal faithful matrix representations of solvable Lie algebras. As application, we have computed a minimal faithful matrix representation for some n-dimensional Lie algebras starting from their laws.

1. PRELIMINARIES

From here on, we have only considered finite-dimensional Lie algebras over the complex number field $\mathbb{C}$. The reader can consult [7] for a comprehensive review on Lie algebras.

Given a Lie algebra $\mathfrak{g}$, its *derived series* is defined as follows

$$\mathcal{C}_1(\mathfrak{g}) = \mathfrak{g},\ \mathcal{C}_2(\mathfrak{g}) = [\mathfrak{g},\mathfrak{g}],\ \mathcal{C}_3(\mathfrak{g}) = [\mathcal{C}_2(\mathfrak{g}),\mathcal{C}_2(\mathfrak{g})],\ \ldots,\ \mathcal{C}_k(\mathfrak{g}) = [\mathcal{C}_{k-1}(\mathfrak{g}),\mathcal{C}_{k-1}(\mathfrak{g})],\ \ldots$$

If there exists a natural integer m such that $\mathcal{C}_m(\mathfrak{g}) \equiv 0$, then $\mathfrak{g}$ is said to be *solvable*. We have the following

Proposition 1.1. *If $\mathfrak{h}$ is a Lie subalgebra of a given Lie algebra $\mathfrak{g}$, then $\mathcal{C}_k(\mathfrak{h}) \subseteq \mathcal{C}_k(\mathfrak{g})$, for all $k \in \mathbb{N}$.*

Given $n \in \mathbb{N}$, the complex solvable Lie algebra $\mathfrak{h}_n$ consists of $n \times n$ upper-triangular matrices; i.e. its elements can be expressed as

$$h_n(x_{r,s}) = \begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ 0 & x_{22} & \cdots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & x_{nn} \end{pmatrix}, \qquad \text{with } x_{r,s} \in \mathbb{C}, \text{ for } 1 \leq r \leq s \leq n.$$

The dimension of $\mathfrak{h}_n$ is $\frac{n(n+1)}{2}$ and the nonzero brackets are

$$\begin{array}{ll} [X_{i,j}, X_{j,k}] = X_{i,k}, & \forall\, 1 \leq i < j < k \leq n; \\ [X_{i,i}, X_{i,j}] = X_{i,j}, & \quad 1 \leq i < j \leq n; \\ [X_{k,i}, X_{i,i}] = X_{k,i}, & \quad \forall\, k \leq i \leq n. \end{array}$$

with respect to the basis $\mathcal{B}_n = \{X_{i,j} = h_n(x_{r,s}) \,|\, x_{r,s} = \delta_{r,i} \cdot \delta_{s,j}, \text{ for } 1 \leq r \leq s \leq n\}_{1 \leq i \leq j \leq n}$, where δ denotes the Krönecker delta function.

2. Minimal Matrix Representations

Given a Lie algebra $\mathfrak{g}$, a *representation* of $\mathfrak{g}$ in $\mathbb{C}^n$ is a Lie-algebra homomorphism $\phi : \mathfrak{g} \to \mathfrak{gl}(\mathbb{C}, n)$. The *dimension* of this representation is the value of $n \in \mathbb{N}$. Ado's theorem assures the existence of a linear injective representation (i.e. a *faithful representation*) on a finite-dimensional vector space for every finite-dimensional Lie algebra over a field of characteristic zero.

Representations are usually defined as $\mathfrak{g}$-*modules*; i.e. Lie-algebra homomorphisms from $\mathfrak{g}$ to Lie algebra $\mathfrak{gl}(V)$ of endomorphisms over an arbitrary n-dimensional vector space V (see [6]).

With respect to minimal representations of Lie algebras, Burde [3] introduced the invariant $\mu(\mathfrak{g})$ for any given Lie algebra $\mathfrak{g}$

$$\mu(\mathfrak{g}) = \min\{\dim(M) \mid M \text{ is a faithful } \mathfrak{g}\text{-module}\}.$$

The goal of this paper is to study matrix faithful representations of solvable Lie algebras. More concretely, we are looking for minimal faithful matrix representations being contained in $\mathfrak{h}_m$, for some $m \in \mathbb{N}$. Indeed, given a solvable Lie algebra $\mathfrak{g}$, our goal is to determine the minimal value m such that $\mathfrak{g}$ is isomorphic to a Lie subalgebra of $\mathfrak{h}_m$, but not of $\mathfrak{h}_{m-1}$. This value is also an invariant of $\mathfrak{g}$ and can be expressed as

$$\bar{\mu}(\mathfrak{g}) = \min\{m \in \mathbb{N} \mid \exists \text{ subalgebra of } \mathfrak{h}_m \text{ isomorphic to } \mathfrak{g}\}.$$

In general, invariants $\mu(\mathfrak{g})$ and $\bar{\mu}(\mathfrak{g})$ can be different from each other.

To carry out the computation of a minimal faithful matrix representations for a given n-dimensional solvable Lie algebra $\mathfrak{g}$ by using Lie algebras $\mathfrak{h}_m$, we have sketched an algorithmic method which only requires the law of $\mathfrak{g}$ as input. The steps of this algorithm are the following

(1) Construct the derived series of $\mathfrak{g}$ and look for the first natural integer k such that this series fits in with that associated with $\mathfrak{h}_k$. Consequently, we are interested in the first k verifying $\mathcal{C}_i(\mathfrak{g}) \subseteq \mathcal{C}_i(\mathfrak{h}_k)$, for all $i \in \mathbb{N}$. This is in virtue of Proposition 1.1.

(2) Express the vectors in the basis $\{e_i\}_{i=1}^n$ of $\mathfrak{g}$ as linear combinations of basis $\mathcal{B}_k$ of $\mathfrak{h}_k$ (i.e. express $\mathfrak{g}$ as a subalgebra of $\mathfrak{h}_k$):

$$e_h = \sum_{1\leq i\leq j\leq k} \lambda_{i,j}^h X_{i,j}, \quad \text{for } 1 \leq h \leq n,$$

taking into account the possible simplifications resulting from Proposition 1.1.

(3) Compute bracket $[e_i, e_j]$ for $1 \leq i \leq j \leq n$ and compare coordinate to coordinate with the results in the laws of $\mathfrak{g}$, but expressed in terms of the basis $\mathcal{B}_k$ of $\mathfrak{h}_k$.

(4) Solve the previous system and consider one of the solutions corresponding to a set of linearly independent vectors (i.e. this solution is the faithful matrix representation searched). If there are no such solutions, then go back to Step 2 and repeat each step with Lie algebra $\mathfrak{h}_{k+1}$ since Lie algebra $\mathfrak{g}$ cannot be represented as a Lie subalgebra of $\mathfrak{h}_k$.

Since we start with $k = 1$ and k increases one unit when there are no representations in $\mathfrak{h}_k$, we can assert that the representation obtained in the previous algorithm is minimal.

3. Some tips for a successful implementation

According to the design previously sketched, the implementation of our procedure should be organized to give answer to the following issues in this order

- Computing the law of solvable Lie algebra $\mathfrak{h}_n$.
- Computing two lists to save the dimension of the ideals in the derived series of $\mathfrak{h}_n$ and $\mathfrak{g}$.
- Determining the minimal dimension k such that the derived series of $\mathfrak{g}$ is compatible with that of $\mathfrak{h}_k$ (i.e. the smallest k which should be considered to find a faithful matrix representation of $\mathfrak{g}$).
- Expressing all the vectors in the basis of $\mathfrak{g}$ as linear combinations of basis $\mathcal{B}_k$ of $\mathfrak{h}_k$.
- Imposing the law of both Lie algebras and applying Proposition 1.1 to obtain an equation system.
- With a symbolic computation package, solving the system of equations resulting from the previous expressions. Since equations are polynomial, every symbolic computation package computes efficiently the algebraic expression of the set of solutions.
- Checking if some of the solutions corresponds to a list of linearly independent vectors.
- If there exists such a solution, then some free coefficients may appear because the faithful matrix representation of $\mathfrak{g}$ may be not unique. In order to obtain a simpler representative, we consider as many null coefficients as possible.

When implementing this algorithm (in our case with Maple), we can compute a minimal faithful matrix representation of any solvable Lie algebra and, more concretely, the list of representations for each dimension whose classification is known.

4. Application to n-dimensional Lie algebras

From a theoretical viewpoint, we want to show how this procedure can be also applied to computing representations for Lie algebras of arbitrary dimension. For example, we have obtained some results regarding the following particular types of algebras

Proposition 4.1. [5, Proposition 3] *If $\mathfrak{s}_n$ is the n-dimensional solvable Lie algebra with basis $\{e_i\}_{i=1}^n$ and law $[e_i, e_n] = e_i$, for $1 \leq i < n$, then $\overline{\mu}(\mathfrak{s}_n) = n$ and a minimal faithful representation of $\mathfrak{s}_n$ is given by $\{e_j = X_{1,j+1}\}_{j=1}^{j=n-1} \cup \{e_n = -X_{1,1}\}$.*

Proposition 4.2. [5, Proposition 4] *If $\mathfrak{H}_{2n+1}$ is the $(2n+1)$-dimensional Heisenberg algebra with basis $\{e_i\}_{i=1}^{2n+1}$ and law $[e_{2i}, e_{2i+1}] = e_1$, for $1 \leq i \leq n$, then $\overline{\mu}(\mathfrak{H}_{2n+1}) = n+2$ and a minimal faithful representation of $\mathfrak{H}_{2n+1}$ is given by $\{e_{2j+1} = X_{j+1,n+2}\}_{j=0}^{j=n} \cup \{e_{2k} = X_{1,k+1}\}_{k=1}^{n+1}$.*

Proposition 4.3. [5, Proposition 5] *If $\mathfrak{f}_n$ is the n-dimensional filiform Lie algebra with basis $\{e_i\}_{i=1}^n$ and law $[e_1, e_h] = e_{h-1}$, for $3 \leq h \leq n$, then $\overline{\mu}(\mathfrak{f}_n) = n$ and a minimal faithful representation of $\mathfrak{f}_n$ is given by $\left\{e_1 = \sum_{i=1}^{n-2} X_{i,i+1}\right\} \cup \{e_j = X_{j-1,n}\}_{j=2}^n$.*

Acknowledgment

This work has been partially supported by MTM2010-19336 and FEDER.
The authors want to thank the referees for their useful comments and suggestions.

References

[1] J. C. Benjumea, F. J. Echarte, J. Núñez and A. F. Tenorio. A method to obtain the Lie group associated with a nilpotent Lie algebra, *Comput. Math. Appl.* **51** (2006) 1493–1506.
[2] J. C. Benjumea, J. Núñez and A. F. Tenorio. Minimal linear representations of the low-dimensional nilpotent Lie algebras, *Math. Scand.* **102** (2008) 17–26.
[3] D. Burde. On a refinement of Ado's Theorem. *Arch. Math. (Basel)* **70** (1998) 118–127.
[4] M. Ceballos, J. Núñez and A. F. Tenorio. Representing Filiform Lie Algebras Minimally and Faithfully by Strictly Upper-Triangular Matrices, *J. Algebra Appl.* **12** (2013), 1250196, 15pp.
[5] M. Ceballos, J. Núñez, A. F. Tenorio. Minimal Faithful Upper-Triangular Matrix Representations for Solvable Lie Algebras, *Submmited* (2014) arXiv:1404.3510 [math.RT]
[6] W. Fulton and J. Harris. *Representation theory: a first course* (Springer-Verlag, 1991).
[7] V. S. Varadarajan. *Lie Groups, Lie Algebras and their Representations*. Selected Monographies **17**, Collæge Press, Beijing, 1998.

University of Seville
E-mail address: mceballos@us.es, jnvaldes@us.es

Pablo de Olavide University
E-mail address: aftenorio@upo.es

ON THE MÖBIUS FUNCTION OF SUBSEMIGROUPS OF $\mathbb{N}$

J. CHAPPELON, I. GARCÍA-MARCO, L. P. MONTEJANO, AND J. L. RAMÍREZ ALFONSÍN

ABSTRACT. Let $\mathcal{S}$ be a subsemigroup of $\mathbb{N}$ and let $(\mathbb{Z}, \leq_{\mathcal{S}})$ be the (locally finite) poset induced by $\mathcal{S}$ on $\mathbb{Z}$ defined by $x \leq_{\mathcal{S}} y$ if and only if $y - x \in \mathcal{S}$ for all $x, y \in \mathbb{Z}$. In this work we investigate $\mu_{\mathcal{S}}$, the Möbius function associated to $(\mathbb{Z}, \leq_{\mathcal{S}})$. In particular, we provide some results relating $\mu_{\mathcal{S}}$ with the Hilbert series of $\mathcal{S}$. As a consequence of these results we are able to describe the Möbius function associated to $(\mathbb{Z}, \leq_{\mathcal{S}})$ when $\mathcal{S}$ is a semigroup with a unique Betti element and when $\mathcal{S}$ is a three generated complete intersection semigroup.

INTRODUCTION

Let $(P, \leq)$ be a *locally finite poset*, i.e., $\leq$ is a partial order for P and for every $x, y \in P$ the set $\{z \in P \,|\, x \leq z \leq y\}$ is finite. Let x and y be elements of P. A chain of length $l \geq 0$ between x and y is a subset of P containing x and y, with cardinality $l + 1$ and totally ordered by $\leq$, that is $\{a_0, a_1, \ldots, a_l\} \subset P$ such that $x = a_0 \lneq a_1 \lneq \cdots \lneq a_l = y$. For any nonnegative integer l, we denote by $c_l(x, y)$ the number of chains of length l between x and y. Note that this number is always finite because the poset P is supposed to be locally finite.

The *Möbius function* μ_P associated to $(P, \leq)$ is the integer-valued function on $P \times P$ defined by

$$\mu_P(x, y) = \sum_{l \geq 0} (-1)^l \, c_l(x, y).$$

The Möbius function is an important concept associated to (locally finite) posets. We refer the reader to [6] for a detailed study and for a large number of applications of the Möbius function.

In this work, we investigate the Möbius function associated to posets arising naturally from subsemigroups of $\mathbb{N}$ as follows. Let $a_1, \ldots, a_n \in \mathbb{N}$ be positive integers and let $\mathcal{S} := \langle a_1, \ldots, a_n \rangle$ denote the subsemigroup of $\mathbb{N}$ generated by $a_1, \ldots, a_n$, that is,

$$\mathcal{S} = \{x_1 a_1 + \cdots + x_n a_n \,|\, x_1, \ldots, x_n \in \mathbb{N}\}.$$

Throughout this work, we consider the structure of poset induced by $\mathcal{S}$ on $\mathbb{Z}$, whose partial order $\leq_{\mathcal{S}}$ is defined by

$$x \leq_{\mathcal{S}} y \iff y - x \in \mathcal{S},$$

for all $x, y \in \mathbb{Z}$. This (locally finite) poset will be denoted by $(\mathbb{Z}, \leq_{\mathcal{S}})$. We denote by $\mu_{\mathcal{S}}$ the Möbius function associated to $(\mathbb{Z}, \leq_{\mathcal{S}})$. For every $x, y \in \mathbb{Z}$ it is easy to check that $\mu_{\mathcal{S}}(x, y) = \mu_{\mathcal{S}}(0, y - x)$. For this reason we only consider the univariate Möbius function $\mu_{\mathcal{S}} : \mathbb{Z} \to \mathbb{Z}$ defined by $\mu_{\mathcal{S}}(x) := \mu_{\mathcal{S}}(0, x)$.

As far as we are aware, the only known results concerning $\mu_{\mathcal{S}}$ is an old theorem due to Deddens [2] that determines the values of $\mu_{\mathcal{S}}$ when $\mathcal{S} = \langle a, b \rangle$, and a recent paper due to Chappelon and Ramírez Alfonsín [1] where the authors investigate $\mu_{\mathcal{S}}$ when $\mathcal{S} = \langle a, a + d, \ldots, a + kd \rangle$ with

$a, k, d \in \mathbb{Z}^+$. In both papers the authors approach the problem by a thorough study of the intrinsic properties of each semigroup.

In this work we present a different and more general approach to the study of $\mu_{\mathcal{S}}$ by means of the Hilbert series of $\mathcal{S}$. As a consequence of this approach we are able to provide formulas for $\mu_{\mathcal{S}}$ when $\mathcal{S}$ belongs to some families of semigroups; namely, when $\mathcal{S}$ is a semigroup with a unique Betti element (yielding to a short proof for Dedden's result) and when $\mathcal{S} = \langle a_1, a_2, a_3 \rangle \subset \mathbb{N}$ is a complete intersection semigroup.

Consider the semigroup $\mathcal{S} = \langle a_1, \ldots, a_n \rangle \subset \mathbb{N}$. We denote by $\mathbb{Z}[[t]]$ the ring of formal power series in the variable t over $\mathbb{Z}$. The Hilbert series associated to $\mathcal{S}$, $H_{\mathcal{S}}(t)$, is

$$H_{\mathcal{S}}(t) := \sum_{b \in \mathcal{S}} t^b \in \mathbb{Z}[[t]].$$

Now we can state the first result, which provides a recursive formula for the Möbius function in terms of the coefficients of $H_{\mathcal{S}}(t)$.

Theorem 1. *If we denote*

$$(1 - t^{a_1}) \cdots (1 - t^{a_n})\, H_{\mathcal{S}}(t) = \sum_{b \in \mathbb{N}} f_b\, t^b \in \mathbb{Z}[t];$$

then, $\sum_{b \in \mathbb{N}} f_b\, \mu_{\mathcal{S}}(x - b) = 0$ *for all* $x \notin \{\sum_{i \in A} a_i \mid A \subset \{1, \ldots, n\}\}$.

We also prove the following.

Theorem 2. $H_{\mathcal{S}}(t)\, \mathcal{G}_{\mathcal{S}}(t) = 1$*, where* $\mathcal{G}_{\mathcal{S}}(t)$ *denotes the generating function of the Möbius function, i.e.,*

$$\mathcal{G}_{\mathcal{S}}(t) := \sum_{b \in \mathbb{N}} \mu_{\mathcal{S}}(b)\, t^b \in \mathbb{Z}[[t]].$$

Hence, the generating function of the Möbius function of $(\mathbb{Z}, \leq_{\mathcal{S}})$ can also be computed as the inverse of the Hilbert series of $\mathcal{S}$.

Thus, Theorems 1 and 2 provide tools to compute the Möbius function of $(\mathbb{Z}, \leq_{\mathcal{S}})$ whenever one knows the Hilbert series of $\mathcal{S}$. We have exploited these results to provide two different proofs of Theorems 3 and 5. In Theorem 3 we provide an explicit formula for $\mu_{\mathcal{S}}$ when $\mathcal{S}$ is a semigroup with a unique Betti element. In Theorem 5 we provide a semi-explicit formula for $\mu_{\mathcal{S}}$ when $\mathcal{S} = \langle a_1, a_2, a_3 \rangle \subset \mathbb{N}$ and $\mathcal{S}$ is a complete intersection.

Every subsemigroup of $\mathbb{N}$ can be described by a finite presentation. Whenever there exists an only $b \in \mathbb{N}$ such that its factorizations give rise to a minimal presentation, then $\mathcal{S}$ is called a *semigroup with a unique Betti element.* These semigroups where studied in detail in [3], where the authors prove that whenever $\mathcal{S} \subset \mathbb{N}$; then, $\mathcal{S} = \langle a_1, \ldots, a_n \rangle$ is a semigroup with a unique Betti element if and only if there exist relatively prime different integers $k_1, \ldots, k_n \geq 2$ such that $a_i := \prod_{j \neq i} k_j$ for all $i \in \{1, \ldots, n\}$. For this family of semigroups the following result holds.

Theorem 3. *Let* $\mathcal{S} = \langle a_1, \ldots, a_n \rangle \subset \mathbb{N}$ *be a semigroup with a unique Betti and denote* $D := \operatorname{lcm}\{a_1, \ldots, a_n\}$*. Then,*

$$\mu_{\mathcal{S}}(x) = \begin{cases} (-1)^{|A|}\binom{k+n-2}{k} & if\ x \geq 0,\ and\ x = \sum_{i \in A} a_i + kD\ with\ A \subset \{1, \ldots, n\}, \\ 0 & otherwise. \end{cases}$$

As a direct consequence of this result we recover Dedden's classical result.

Corollary 4. *Let $a, b \in \mathbb{Z}^+$ be relatively prime integers and consider $\mathcal{S} := \langle a, b\rangle$. Then,*

$$\mu_{\mathcal{S}}(x) = \begin{cases} 1 & if\ x \geq 0\ and\ x \equiv 0\ or\ a+b \pmod{ab}, \\ -1 & if\ x \geq 0\ and\ x \equiv a\ or\ b \pmod{ab}, \\ 0 & otherwise. \end{cases}$$

Now we present a semi-explicit formula for the Möbius function of $\mathcal{S}$ when $\mathcal{S} = \langle a_1, a_2, a_3\rangle$ is a complete intersection semigroup and $\gcd\{a_1, a_2, a_3\} = 1$. In this setting we know from [4] that $\mathcal{S}$ is a complete intersection if and only if $\gcd\{a_i, a_j\}\, a_k \in \langle a_i, a_j\rangle$ with $\{i, j, k\} = \{1, 2, 3\}$; we assume that $\gcd\{a_2, a_3\}\, a_1 \in \langle a_2, a_3\rangle$ and denote $d := \gcd\{a_2, a_3\}$.

In order to present Theorem 5 we need to introduce the notion of the Sylvester denumerant $d_B(x)$ for $B = (b_1, \ldots, b_k) \in \mathbb{N}^k$, which is the number of non-negative integer solutions $(x_1, \ldots, x_k) \in \mathbb{N}^k$ to the equation $x = \sum_{i=1}^k x_i b_i$.

Theorem 5. *Let $\mathcal{S} = \langle a_1, a_2, a_3\rangle$ be a numerical semigroup such that $da_1 \in \langle a_2, a_3\rangle$ where $d := \gcd\{a_2, a_3\}$. Then, for every $x \in \mathbb{Z}$ there exists a unique $\alpha \in \{0, \ldots, d-1\}$ such that $x = \alpha a_1 + x'$ and $d \mid x'$; moreover,*

$$\mu_{\mathcal{S}}(x) = 0$$

if $\alpha \geq 2$, or

$$\mu_{\mathcal{S}}(x) = (-1)^{\alpha} \left(d_B(x') - d_B(x' - a_2) - d_B(x' - a_3) + d_B(x' - a_2 - a_3)\right)$$

otherwise, where $B := (da_1, a_2\, a_3/d)$.

Hence, this result expresses the Möbius function associated to $(\mathbb{Z}, \leq_{\mathcal{S}})$, where $\mathcal{S}$ is a three generated complete intersection numerical semigroup, in terms of a unique writing of every integer and of four Sylvester denumerants of the form $d_B(y)$, where $B = (p, q)$. These denumerants can be computed following the results in [5, Chapter 4.4]. More precisely, if we set $d := \gcd\{p, q\}$, one can compute $d_B(y)$ with the following formula:

$$(1)\qquad d_B(y) = \begin{cases} 0 & if\ d \nmid y, \\ & \\ d_{B'}(y/b) & if\ d > 1\ and\ d \mid y;\ where\ B' := (p/d, q/d), \\ & \\ \frac{y+pp'+qq'}{pq} - 1 & \text{o}therwise;\ where\, p' \in \{1, \ldots, q\},\ q' \in \{1, \ldots, p\}, \\ & q \mid (pp' + y),\ and\, p \mid (qq' + y). \end{cases}$$

Thus, Theorem 5 yields an algorithm to compute $\mu_{\mathcal{S}}(x)$ for $x \in \mathbb{Z}$ in this setting. In the resulting algorithm one firstly determines if $\alpha = 0$, $\alpha = 1$ or $\alpha \geq 2$; we observe that $\alpha = 0$ if $d \mid x$, $\alpha = 1$ if $d \mid x - a_1$ and $\alpha \geq 2$ otherwise. If $\alpha \geq 2$, then $\mu_{\mathcal{S}}(x) = 0$ and we are done. If $\alpha \in \{0, 1\}$, then we set $x' := x - \alpha a_1$ and follow (1) to compute $d_B(x'), d_B(x' - a_2), d_B(x' - a_3)$ and $d_B(x' - a_2 - a_3)$, where $B := (da_1, a_2\, a_3/d)$. Finally, we return the result obtained after substituting the corresponding values in the formula given in Theorem 5.

REFERENCES

[1] J. Chappelon and J. L. Ramírez Alfonsín, On the Möbius function of the locally finite poset associated with a numerical semigroup, Semigroup Forum **87**, 313–330 (2013),

[2] J. A. Deddens, A combinatorial identity involving relatively prime integers, J. Comb. Theory, Ser. A **26**, 189–192 (1979).

[3] P. A. García-Sánchez, I. Ojeda and J. C. Rosales, Affine semigroups having a unique Betti element, J. Algebra Appl. **12** (2013), no. 3, 1250177, 11 pp.

[4] J. Herzog, Generators and relations of abelian semigroups and semigroup rings, Manuscripta Math. **3** (1970), 175–193.

[5] J. L. Ramírez Alfonsín, *The Diophantine Frobenius Problem*, Oxford Lecture Series in Mathematics and Its Applications, vol. 30. Oxford University Press, Oxford (2005).

[6] G. C. Rota, On the foundations of combinatorial theory I. Theory of Möbius functions, Z. Wahrscheinlichkeitstheor. **2**, 340–368 (1964).

Unviersité Montpellier 2. Insitut de Mathématiques et de Modélistation de Montpellier (I3M)
Place Eugène Bataillon
34095 Montpellier Cedex, France

E-mail address: jonathan.chappelon@univ-montp2.fr, ignacio.garcia-marco@univ-montp2.fr, luis.pedro.montejano@upc.edu, jramirez@math.univ-montp2.fr.

SOME STABILITY PHENOMENA FOR THE REDUCED KRONECKER COEFFICIENTS.

LAURA COLMENAREJO AND MERCEDES ROSAS

ABSTRACT. The reduced Kronecker coefficients are a family of integers closely related to the decomposition into irreducibles of both the general lineal group and the symmetric group. In this work we investigate certain sequences of reduced Kronecker coefficients $\bar{g}_{k\mu,k\nu}^{k\lambda+(i)}$, depending of k and i. We show that have interesting stabilization properties.

1. INTRODUCTION

A central theme in mathematics is the idea of symmetry. First and foremost, symmetries are encoded using the symmetric groups and the complex general lineal groups. The representation theory of these groups are deeply intertwined by the famous Schur-Weyl duality.

Given two irreducible representations of a group, an important problem asks how to decompose their tensor product into irreducibles. For the general linear group $GL(k, \mathbb{C})$ the beautiful combinatorics surrounding the Littlewood–Richardson coefficients explains us how to achieve this decomposition. It develops that the irreducible representations of the general lineal group are labelled by integer partitions λ, with $\ell(\lambda) \leq k$. The Littlewood–Richardson coefficients $c_{\mu,\nu}^{\lambda}$ are indexed by triples of partitions μ, ν, and λ, with $|\mu| + |\nu| = |\lambda|$.

For the symmetric group $\mathbb{S}_n$, the multiplicities appearing in the decomposition of the tensor product of irreducible representations are called the Kronecker coefficients. The irreducible representations of the $\mathbb{S}_n$ are indexed by partitions of n. The Kronecker coefficients $g_{\mu,\nu}^{\lambda}$ are indexed by triples of partitions μ, ν, and λ, with $|\mu| = |\nu| = |\lambda| = n$.

Trying to understand the Kronecker coefficients is a problem that has captured the attention of mathematicians for more than a century, but that has remained unsolved. Recently, it has come back to the forefront because of their connections to geometric complexity theory and to quantum information theory.

In 1938 Murnaghan discovered an intriguing stabilization phenomena for the Kronecker coefficients, [5]. They stabilize when we increase the first rows of its three indexing partitions. The limits of these sequences are known as the reduced Kronecker coefficients. They are indexed by the partitions obtained after deleting the first parts of the original triple. Note that the resulting partitions do not have to add to the same number. Indeed, as observed by Littlewood if the resulting partitions satisfy that $|\mu| + |\nu| = |\lambda|$, then the reduced Kronecker coefficients coincide with the Littlewood-Richardson coefficients.

The reduced Kronecker coefficients $\bar{g}_{\mu,\nu}^{\lambda}$ have been shown to govern the representation theory of the partition algebra, [1]. They are believed to simpler the Kronecker coefficients, but their knowledge suffices to compute the Kronecker coefficient, [2]. Kirillov and Klyachko, [3, 4], have conjectured that the reduced Kronecker coefficients satisfy the saturation hypothesis : For any $k \geq 1$ we have that $\bar{g}_{k\mu,k\nu}^{k\lambda} > 0$ iff $\bar{g}_{\mu,\nu}^{\lambda} > 0$. This is known not to be the case for the Kronecker coefficients.

In this abstract we investigate a related family of sequences of reduced Kronecker coefficients $\bar{g}_{k\mu,k\nu}^{k\lambda+(i)}$, depending k and i. We give partial evidence that their behavior is consistent with the idea that they count integer points in some polytope. We show the saturation conjecture holds, when applicable. We also show the occurrence of new limiting phenomenon reminiscent of the one described for Murnaghan for the reduced Kronecker coefficients.

Both authors have been partially supported by projects MTM2010-19336, FEDER, and FQM333 of the Spanish government.

2. Linearity : three one-row partitions.

Using SAGE, we tested the saturation hypothesis for the reduced Kronecker coefficients. We focus on the family $\mu = (a)$, $\nu = (b)$ and $\lambda = (c)$, and add a fixed partition (i) to introduce an affine twist. The results obtained show the existence of new stabilization phenomena. We present our results using some of examples, and then give formulas that describe our observations in full generality. The formulas follow from Theorem 2.4.

Let $\lfloor a \rfloor$, be the largest integer less than or equal to a. For the tables, we follow the convention that the columns are indexed by k and the rows by i.

Example 2.1 (Stabilization among the diagonals)**.** Consider sequences of reduced Kronecker coefficients $\bar{g}_{(k),(k)}^{(k+i)}$:

$$\begin{array}{ccccccccccccccc}
\mathbf{1}, & 1, & 2, & 2, & \mathbf{3}, & 3, & 4, & 4, & 5, & \mathbf{5}, & 6, & 6, & 7, & 7, & 8, \\
0, & \mathbf{1}, & 1, & 2, & 2, & \mathbf{3}, & 3, & 4, & 4, & 5, & \mathbf{5}, & 6, & 6, & 7, & 7, \\
0, & 0, & \mathbf{1}, & 1, & 2, & 2, & \mathbf{3}, & 3, & 4, & 4, & 5, & \mathbf{5}, & 6, & 6, & 7, \\
0, & 0, & 0, & \mathbf{1}, & 1, & 2, & 2, & \mathbf{3}, & 3, & 4, & 4, & 5, & \mathbf{5}, & 6, & 6, \\
0, & 0, & 0, & 0, & \mathbf{1}, & 1, & 2, & 2, & \mathbf{3}, & 3, & 4, & 4, & 5, & \mathbf{5}, & 6, \\
0, & 0, & 0, & 0, & 0, & \mathbf{1}, & 1, & 2, & 2, & \mathbf{3}, & 3, & 4, & 4, & 5, & \mathbf{5}, \\
0, & 0, & 0, & 0, & 0, & 0, & \mathbf{1}, & 1, & 2, & 2, & \mathbf{3}, & 3, & 4, & 4, & 5, \\
0, & 0, & 0, & 0, & 0, & 0, & 0, & \mathbf{1}, & 1, & 2, & 2, & \mathbf{3}, & 3, & 4, & 4
\end{array}$$

The coefficients in the i^{th} diagonal, $\bar{g}_{(k),(k)}^{(2k-i)}$, stabilize to $\lfloor \frac{i}{2} \rfloor + 1$ when k grows. The nonzero entries in the i^{th} diagonal, $\bar{g}_{(k),(k)}^{(k+i)}$, are constant.

Example 2.2. Consider now the family of reduced Kronecker coefficients $\bar{g}_{(k),(k)}^{(i)}$. The rows start being zero. Then, they grow linearly, to finally they stabilize in a value that only depends on i, as in the previous example.

$$\begin{array}{cccccccccccccc}
\mathbf{1}, & 1, & 1, & 1, & 1, & 1, & 1, & 1, & 1, & 1, & 1, & 1, & 1, & 1, \\
0, & \mathbf{1}, & 1, & 1, & 1, & 1, & 1, & 1, & 1, & 1, & 1, & 1, & 1, & 1, \\
0, & 1, & \mathbf{2}, & 2, & 2, & 2, & 2, & 2, & 2, & 2, & 2, & 2, & 2, & 2, \\
0, & 0, & 1, & \mathbf{2}, & 2, & 2, & 2, & 2, & 2, & 2, & 2, & 2, & 2, & 2, \\
0, & 0, & 1, & 2, & \mathbf{3}, & 3, & 3, & 3, & 3, & 3, & 3, & 3, & 3, & 3, \\
0, & 0, & 0, & 1, & 2, & \mathbf{3}, & 3, & 3, & 3, & 3, & 3, & 3, & 3, & 3, \\
0, & 0, & 0, & 1, & 2, & 3, & \mathbf{4}, & 4, & 4, & 4, & 4, & 4, & 4, & 4, \\
0, & 0, & 0, & 0, & 1, & 2, & 3, & \mathbf{4}, & 4, & 4, & 4, & 4, & 4, & 4,
\end{array}$$

This is a general phenomena: if we consider any family of coefficients of this form such that $a = b + c$, then

$$\bar{g} = \begin{cases} 0 & 0 \leq k < \frac{i}{2b} \\ \lfloor \frac{2bk-i}{2} \rfloor + 1 & \frac{i}{2b} \leq k \leq \frac{i}{b} \\ \lfloor \frac{i}{2} \rfloor + 1 & k > \frac{i}{b} \end{cases}$$

Observe that for i, the family of coefficients stabilizes to $\lfloor \frac{i}{2} \rfloor + 1$.

There is just another possible situation. If we make $\mu = (2)$, we observe another phenomena consistent with the idea that, as for the Littlewood-Richardson coefficients, the reduced Kronecker coefficients count the number of integral point on a polytope.

Example 2.3. For the sequences $\bar{g}^{(i)}_{(2k),(k)}$ we obtain :

$$\begin{array}{cccccccccccccc}
\mathbf{1}, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, \\
0, & \mathbf{1}, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, \\
0, & \mathbf{1}, & \mathbf{1}, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, \\
0, & \mathbf{1}, & \mathbf{1}, & \mathbf{1}, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, \\
0, & 0, & \mathbf{2}, & \mathbf{1}, & \mathbf{1}, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, \\
0, & 0, & \mathbf{1}, & \mathbf{2}, & \mathbf{1}, & \mathbf{1}, & 0, & 0, & 0, & 0, & 0, & 0, & 0, & 0, \\
0, & 0, & \mathbf{1}, & \mathbf{2}, & \mathbf{2}, & \mathbf{1}, & \mathbf{1}, & 0, & 0, & 0, & 0, & 0, & 0, & 0, \\
0, & 0, & 0, & \mathbf{2}, & \mathbf{2}, & \mathbf{2}, & \mathbf{1}, & \mathbf{1}, & 0, & 0, & 0, & 0, & 0, & 0,
\end{array}$$

At each row, and after some zeroes, we have that the entries increase linearly, and after reaching its maximum value, they decrease linearly to zero. Indeed, this family of coefficients stabilize to zero for all i.

This is a particular example of the following fact. If $c = 0, b = 1$ and $a \geq 2$ then

$$\bar{g} = \begin{cases} 0 & 0 \leq k < \frac{i}{a+1} \\ \lfloor \frac{(a+1)k-i}{2} \rfloor + 1 & \frac{i}{a+1} \leq k \leq \frac{i}{a} \\ \lfloor \frac{i-(a-1)k}{2} \rfloor + 1 & \frac{i}{a} \leq k \leq \frac{i}{a-1} \\ 0 & k > \frac{i}{a-1} \end{cases}$$

We can see that they stabilize to 0 and they have a maximum at $k = \lfloor \frac{i}{a} \rfloor$ with value $\lfloor \frac{i-(a-1)k}{2} \rfloor +$ 1.

We say that $f : \mathbb{N} \to \mathbb{Z}$ is a quasi-polynomial if there exists a period m and polynomials $p_i \in \mathbb{Z}[t]$ such that $f(t) = p_i(t)$ for $t \equiv i \mod m$.

Theorem 2.4. *Fix $\mu = (a), \nu = (b)$, and $\lambda = (c)$. Then, the value of the reduced Kronecker coefficient $\bar{g}^{k\lambda+(i)}_{k\mu,k\nu}$ is given by a piecewise linear polynomial P of period 2.*

Moreover, the asymptotic behavior of the quasi-polynomial corresponds always to one of the examples given above.

We have explicit formulas for this piecewise linear quasi polynomial (that depends on μ, ν and λ fixed). In this abstract we only include a portion of it. The proof of the theorem is based on the translation for reduced Kronecker coefficients of the results obtained in [6] for the case when the Kronecker coefficients are of the form $\{g^{\lambda}_{\mu\nu} : \mu = (\mu_1, \mu_2)\ \nu = (\nu_1, \nu_2)\}$.

3. A NONLINEAR EXAMPLE

The fact that for the families considered about, the reduced Kronecker coefficients are given by linear quasi polynomials is a consequence of the fact that the three indexing partitions μ, ν and λ have only one part. We are currently investigating what happens in general. While the coefficients do not grow linearly, the presence of new stabilization phenomena seems to be a general fact. We close this abstract with the following elegant observation. The sequences $\bar{g}^{(k)}_{(k,k),(k+i,k)}$ stabilize to the sequence $\frac{1}{(1-x)^2(1-x^2)^2(1-x^3)}$ when i grows.

1,	3,	4,	7,	9,	14,	17,	24,	29	38	45	57	66	81,	93	$A008763$
1,	**2**,	4,	7,	11,	16,	23,	31,	41,	53,	67,	83,	102,	123,	147	$A000601$
0,	**1**,	**2**,	**5**,	8,	14,	20,	30,	40,	55,	70,	91,	112,	140,	168	$A006918$
0,	0,	**1**,	**2**,	**5**,	**9**,	15,	23,	34,	47,	64,	84,	108,	136,	169	$A014126$
0,	0,	0,	**1**,	**2**,	**5**,	**9**,	**16**,	24,	37,	51,	71,	93,	122,	153	
0,	0,	0,	0,	**1**,	**2**,	**5**,	**9**,	**16**,	**25**,	38,	54,	75,	100,	131	$A175287$
0,	0,	0,	0,	0	**1**,	**2**,	**5**,	**9**,	**16**,	**25**,	**39**,	55,	78	104	
0,	0,	0,	0,	0,	0	**1**,	**2**,	**5**,	**9**,	**16**,	**25**,	**39**,	**56**,	79	

Indeed, if we disregard the starting zeroes, i.e., we look at $\bar{g}^{(k)}_{(k,k),(2k-i,k)}$, we obtain a sequence of sequences that converges to

$$\frac{1}{(1-x)^2(1-x^2)^2(1-x^3)} = 1, 2, 5, 9, 16, 25, 39, 56, 80, 109, 147, 192, 249, 315, 396, \cdots$$

Furthermore, at each row (at each value of i) the first nonzero i terms of $\bar{g}^{(k)}_{(k,k),(2k-i,k)}$ are identical with the first entries of $\frac{1}{(1-x)^2(1-x^2)^2(1-x^3)}$.

REFERENCES

[1] C. Bowman, M. De Visscher and R. Orellana, The partition algebra and the Kronecker coefficients to appear in Transactions of the American Mathematical Society.

[2] Briand, Emmanuel; Orellana, Rosa; Rosas, Mercedes The stability of the Kronecker product of Schur functions. J. Algebra 331 (2011), 11–27.

[3] Klyachko, A, Quantum marginal problem and representations of the symmetric group, arXiv:quant-ph/0409113, September 2004.

[4] Kirillov, Anatol N. An invitation to the generalized saturation conjecture. Publ. Res. Inst. Math. Sci. 40 (2004), no. 4, 1147–1239.

[5] Murnaghan, Francis The analysis of the Kronecker product of irreducible representations of the symmetric group, Amer. J. Math. 60 (3) (1938) 761–784.

[6] Rosas, Mercedes H. The Kronecker product of Schur functions indexed by two-row shapes or hook shapes. J. Algebraic Combin. 14 (2001), no. 2, 153–173.

LAURA COLMENAREJO. Departamento de Álgebra. Universidad de Sevilla.
E-mail address: laurach@us.es

MERCEDES ROSAS. Departamento de Álgebra. Universidad de Sevilla.
E-mail address: mrosas@us.es

ZIGZAG FORM OVER FAMILIES OF PARAMETRIC MATRICES

ROBERT M. CORLESS, MARC MORENO MAZA, AND STEVEN E. THORNTON

INTRODUCTION

This work was initially motivated by a desire to compute the Frobenius (rational) canonical forms of parametric matrices for applications in dynamical system theory. The Frobenius form can easily be extended to the Jordan and Weyr (see [11]) canonical forms. Additionally, the minimal polynomial is easily extracted form the Frobenius form.

Currently, computations on parametric matrices are considered difficult and costly because canonical forms such as the Frobenius, Jordan and Weyr forms are discontinuous; this requires special cases for completeness, and exhaustive analysis produces combinatorially many cases. Some papers considering special cases with parameters include [1] and [5].

There are a large number of methods for computing the Frobenius form of a constant matrix such as in [2], [7], [8], [9], [10] and [12]. We instead modify the algorithm of Storjohann from [13] and [14] for computations on parametric matrices. This algorithm requires the computation of the so-called *Zigzag form* before the Frobenius form can be computed. The Zigzag form itself is not directly useful for applications but provides a matrix from which the Frobenius form can easily be obtained. This will be discussed in detail in a forthcoming paper.

We begin by introducing the algebraic material necessary for the computation. Section 2 introduces the concept of a parametric Zigzag matrix. Section 3 briefly describes the algorithm for computing the set of Zigzag matrices similar to a parametric matrix as an extension of [13]. We then briefly describe how this algorithm has been implemented with the `RegularChains` library, in Section 4. We finish off by considering future work.

1. PRELIMINARIES

Let $\mathbb{K}$ be an algebraically closed field or a real closed field. Let $\alpha_1 < \cdots < \alpha_m$ be $m \geq 1$ ordered variables. We denote by $\mathbb{K}[\alpha] = \mathbb{K}[\alpha_1, \ldots, \alpha_m]$ the ring of polynomials in the variables $\alpha = \alpha_1, \ldots, \alpha_m$ with coefficients in $\mathbb{K}$. We denote by $\mathbb{K}(\alpha)$ the quotient field of $\mathbb{K}[\alpha]$, that is, the field of multivariate rational functions in α with coefficients in $\mathbb{K}$.

Constructible Set. If $\mathbb{K}$ is algebraically closed, we call a *constructible set* S of $\mathbb{K}[\alpha]$ the solution set of any polynomial system of the form

$$f_1(\alpha) = \cdots = f_a(\alpha) = 0,\ g(\alpha) \neq 0 \tag{1}$$

where $f_1(\alpha), \ldots, f_a(\alpha), g(\alpha)$ are polynomials of $\mathbb{K}[\alpha]$. If $f_1(\alpha), \ldots, f_a(\alpha)$ form a *regular chain* of $\mathbb{K}[\alpha]$ (see [4]) and if the polynomial $g(\alpha)$ is regular (i.e. neither zero nor a zero-divisor) modulo the saturated ideal of this regular chain, then the system (1) is called a *regular system* (see [6]). When this holds, we necessarily have $S \neq \varnothing$.

Semi-Algebraic Set. If $\mathbb{K}$ is a real closed field, we call a *semi-algebraic set* S of $\mathbb{K}[\alpha]$ the solution set of any polynomial system of the form

$$f_1(\alpha) = \cdots = f_a(\alpha) = 0,\ g(\alpha) \neq 0,\ p_1(\alpha) > 0, \ldots, p_b(\alpha) > 0,\ q_1(\alpha) \geq 0, \ldots, q_c(\alpha) \geq 0$$

where $f_1(\alpha), \ldots, f_a(\alpha), g(\alpha), p_1(\alpha), \ldots, p_b(\alpha), q_1(\alpha), \ldots, q_c(\alpha)$ are polynomials of $\mathbb{K}[\alpha]$. Under some additional technical assumptions (in particular assuming that $f_1(\alpha), \ldots, f_a(\alpha)$ is a regular chain and that each of the polynomial $p_1(\alpha), \ldots, p_b(\alpha)$ is regular modulo the saturated ideal of this regular chain, see [3]) then the system (1) is called a *regular semi-algebraic system.* When this holds, we necessarily have $S \neq \varnothing$.

Proposition 1.1 ([6, 3])**.** *Assume $\mathbb{K}$ is algebraically closed (resp. real closed). Then, for every constructible set (resp. semi-algebraic set) $S \subseteq \mathbb{K}^m$ one can compute finitely many regular systems (resp. regular semi-algebraic system) $\Sigma_1, \ldots, \Sigma_\ell$ such that the union of their solution sets equals S; we call $\Sigma_1, \ldots, \Sigma_\ell$ a* triangular decomposition *of S. Moreover, for two construtible sets (resp. semi-algebraic sets) $S_1, S_2 \subset \mathbb{K}^m$, one can compute a triangular decomposition of their intersection $S_1 \cap S_2$, their union $S_1 \cup S_2$ and the set theoretical difference $S_1 \setminus S_2$.*

Remark 1.2. Let $S \subseteq \mathbb{K}^m$ be a constructible (resp. semi-algebraic) set and $f(\alpha) \in \mathbb{K}[\alpha]$. A useful tool for later computations will be finding the partition $(S_{\mathrm{eq}}, S_{\mathrm{neq}})$ of S defined by

$$S_{\mathrm{eq}} \ = \ S \cap V(f(\alpha)) \ \text{ and } \ S_{\mathrm{neq}} \ = \ S \setminus V(f(\alpha)) = S \setminus S_{\mathrm{eq}}$$

by means of the algorithms of [6, 3].

2. Zigzag Matrix

Parametric Polynomial. Let x be an additional variable. Let $f(x;\alpha)$ be a monic polynomial of degree r w.r.t. x. We write:

$$f(x;\alpha) = f_0(\alpha) + f_1(\alpha)x + \cdots + f_{r-1}(\alpha)x^{r-1} + x^r \tag{2}$$

where the *coefficients* $f_0(\alpha), \ldots, f_{r-1}(\alpha)$ are rational functions in $\mathbb{K}(\alpha)$. We assume that the values of α are constrained to belong to a constructible (resp. semi-algebraic) set S. In particular, the denominator of every coefficient $f_0(\alpha), \ldots, f_{r-1}(\alpha)$ is nonzero everywhere on S. This can be achieved thanks to Proposition 1.1.

Companion Matrix. The *Frobenius companion matrix* in x of the polynomial in Equation (2) takes the form

$$C_{f(x;\alpha)} = \begin{bmatrix} 0 & \cdots & 0 & -f_0(\alpha) \\ 1 & \ddots & \vdots & \vdots \\ & \ddots & 0 & -f_{r-2}(\alpha) \\ & & 1 & -f_{r-1}(\alpha) \end{bmatrix} \tag{3}$$

where the values of α are restricted by the set S as above.

Remark 2.1. $f(x;\alpha)$ may be expressed in bases other than the monomial, and other forms of companion matrices exist and are useful.

Zigzag Matrix. A parametric *Zigzag matrix* takes the form

$$\begin{bmatrix}
C_{c_1(x;\alpha)} & B_{b_1} & & & & & & \\
 & C^T_{c_2(x;\alpha)} & & & & & & \\
 & B_{b_2} & C_{c_3(x;\alpha)} & B_{b_3} & & & & \\
 & & & C^T_{c_4(x;\alpha)} & & & & \\
 & & & & \ddots & & & \\
 & & & & & C^T_{c_{k-2}(x;\alpha)} & & \\
 & & & & & B_{b_{k-2}} & C_{c_{k-1}(x;\alpha)} & B_{b_{k-1}} \\
 & & & & & & & C^T_{c_k(x;\alpha)}
\end{bmatrix} \tag{4}$$

for k even. Each polynomial $c_1(x;\alpha), \ldots, c_k(x;\alpha)$ takes the same form as Equation (2). Again, we restrict the values of α by the above set S such that the denominator of every coefficient of $c_1(x;\alpha), \ldots, c_k(x;\alpha)$ is non-zero everywhere on S. The B_{b_i} blocks are zero matrices with either a 0 or 1 in the upper left entry and their size is determined by their neighbouring companion blocks.

To cover the case where there may be an odd number of blocks along the diagonal (k odd), the conditions $\deg c_i \geq 1$ for $1 \leq i < k$ and $\deg c_k \geq 0$ are introduced. This allows the kth diagonal block to have dimension zero and hence the block $B_{b_{k-1}}$ above $C^T_{c_k(x;\alpha)}$ will also have dimension zero.

3. Computation

The algorithm discussed in this section extends the work of Storjohann in [13] and [14] to the computation of Zigzag forms of families of parametric matrices.

Theorem 3.1. *Let $\mathbb{K}$, $\mathbb{K}[\alpha]$ and S be as in Section 1. For every matrix $A(\alpha) \in \mathbb{K}^{n\times n}[\alpha]$, there exists a partition $(S_1, \ldots, S_N)$ of S such that for each S_i, there exists a matrix $Z_i(\alpha) \sim A(\alpha)$ in Zigzag form where the denominators of the coefficients of the entries of $Z_i(\alpha)$ are all non-zero everywhere on S_i.*

We follow the same algorithm presented in Section 2 of [13]. Stages 1 and 3 must be modified for finding pivots vanishing nowhere on the underlying constructible (resp. semi-algebraic) set. Proposition 1.1 tells us that this can be achieved and Remark 1.2 emphasizes the fact that this can lead to generate a case discussion, which is a standard procedure in the computation of triangular decompositions. Once computation has split into two branches, one where a pivot has been found and the set S has been replaced with S_{neq}, and another where the pivot has not yet been found and the search for a pivot continues with S replaced by S_{eq}, the computations proceed in parallel (or by stack execution sequentially).

4. Implementation

A sequential implementation has been written in MAPLE to compute the set of Zigzag forms similar to an input parametric matrix under algebraic or semi-algebraic constraints. The `RegularChains` library in MAPLE contains many useful procedures and sub-packages for performing polynomial computations with parameters. See `www.regularchains.org` for details. The `ConstructibleSetTools` and `SemiAlgebraicSetTools` sub-packages of `RegularChains` are useful for representing constructible sets and semi-algebraic sets respectively and, performing set operations on them, as mentioned in Proposition 1.1. The `GeneralConstruct` procedure from the `ConstructibleSetTools` obtains a triangular decomposition of an input system of polynomial equations and inequations. Analogously, the `RealTriangularize` procedure computes a triangular decomposition of a semi-algebraic set given by an input system of polynomial equations, inequations and inequalities. The intersection and set theoretical difference computations needed in remark 1.2 are performed by the `Intersection` and `Difference` commands of the `ConstructibleSetTools` and `SemiAlgebraicSetTools` sub-packages.

Cost. As one can expect, we have verified experimentally that the main cost of the implemented algorithm comes from the computations of the intersections needed in remark 1.2. Clearly, this costs grows exponentially with the number m of parameters $\alpha_1, \dots, \alpha_m$.

Example 4.1. Consider the 3×3 matrix with a single parameter α over the complex numbers $\mathbb{C}$

$$A(\alpha) = \begin{bmatrix} -1 & -\alpha - 1 & 0 \\ -1/2 & \alpha - 2 & 1/2 \\ -2 & 3\alpha + 1 & -1 \end{bmatrix}$$

with no input conditions on α. The Zigzag forms similar to this matrix are

$$Z_1(\alpha) = \begin{bmatrix} 0 & 0 & 4\alpha \\ 1 & 0 & 4(\alpha - 1) \\ 0 & 1 & \alpha - 4 \end{bmatrix} \quad \alpha + 3 \neq 0, \quad Z_2(\alpha) = \left[\begin{array}{cc|c} 0 & -4 & 1 \\ 1 & -4 & 0 \\ \hline 0 & 0 & -3 \end{array}\right] \quad \alpha + 3 = 0\,.$$

Clearly, $Z_1(\alpha)$ is already in Frobenius form whereas $Z_2(\alpha)$ requires additional work to obtain the Frobenius form. This example turns out to have a continuous Frobenius form in the parameter, hence the Frobenius form is $Z_1(\alpha)$ for all values of α.

Using the MAPLE implementation written, this could be computed by executing the MAPLE code (replacing α by a):

```
> with(RegularChains):
> with(ConstructibleSetTools):
> R := PolynomialRing([a]):
> S := GeneralConstruct([],[],R):
> A := Matrix([[-1, -a-1, 0],[-1/2, a-2, 1/2],[-2, 3*a+1, -1]]):
> Z := ParametricZigzagForm(A, S, R);
```

5. APPLICATIONS

The implementation code together with a variety of test examples of various levels of difficulty can be downloaded from `http://steventhornton.ca/coderepository/`. In particular, some examples are taken from the literature on control system design where parametric matrices arise. We are currently extending the functionalities offered by this implementation dedicated to parametric matrices under algebraic or semi-algebraic constraints. Indeed, from the Zigzag form, the Frobenius form can easily be determined, leading to the computation of the Jordan form and the minimal polynomial.

References

[1] V. I. Arnold. On matrices depending on parameters. *Russian Mathematical Surveys*, 26(2):29–43, 1971.

[2] D. Augot and P. Camion. On the computation of minimal polynomials, cyclic vectors, and Frobenius forms. *Linear Algebra and its Applications*, 260:61–94, 1997.

[3] C. Chen, J. H. Davenport, J. P. May, M. Moreno Maza, B. Xia, and R. Xiao. Triangular decomposition of semi-algebraic systems. *J. Symb. Comput.*, 49:3–26, 2013.

[4] C. Chen and M. Moreno Maza. Algorithms for computing triangular decomposition of polynomial systems. *J. Symb. Comput.*, 47(6):610–642, 2012.

[5] G. Chen. Computing the normal forms of matrices depending on parameters. In *Proceedings of ISSAC-89, Portland, Oregon*, pages 244–249. ACM Press-Addison Wesley, 1989.

[6] V. G. Ganzha, E. W. Mayr, and E. V. Vorozhtsov, editors. *Computer Algebra in Scientific Computing, 10th International Workshop, CASC 2007, Bonn, Germany, September 16-20, 2007, Proceedings*, volume 4770 of *Lecture Notes in Computer Science*. Springer, 2007.

[7] M. Giesbrecht. Fast algorithms for matrix normal forms. In *Foundations of Computer Science, 1992. Proceedings., 33rd Annual Symposium on*, pages 121–130. IEEE, 1992.

[8] M. Giesbrecht. Nearly optimal algorithms for canonical matrix forms. *SIAM Journal on Computing*, 24(5):948–969, 1995.

[9] E. Kaltofen, M. S. Krishnamoorthy, and B. David Saunders. Parallel algorithms for matrix normal forms. *Linear Algebra and its Applications*, 136:189–208, 1990.

[10] K. R. Matthews. A rational canonical form algorithm. *Mathematica Bohemica*, 117(3):315–324, 1992.

[11] K. O'Meara, J. Clark, and C. Vinsonhaler. *Advanced Topics in Linear Algebra: Weaving Matrix Problems Through the Weyr Form*. Oxford University Press, 2011.

[12] P. Ozello. *Calcul exact des formes de Jordan et de Frobenius d'une matrice*. PhD thesis, Université Joseph-Fourier-Grenoble I, 1987.

[13] A. Storjohann. An $\mathcal{O}(n^3)$ algorithm for the Frobenius normal form. In *Proceedings of the 1998 international symposium on Symbolic and algebraic computation*, pages 101–105. ACM, 1998.

[14] A. Storjohann. Algorithms for matrix canonical forms. *These de doctorat, Institut für Wissenschaftliches Rechnen, ETH-Zentrum, Zürich, Switzerland*, 2000.

Ontario Research Centre for Computer Algebra, Western University, London, Canada
E-mail address: `rcorless@uwo.ca`
E-mail address: `moreno@csd.uwo.ca`
E-mail address: `sthornt7@uwo.ca`

THE REES ALGEBRA OF A MONOMIAL PLANE PARAMETRIZATION

TERESA CORTADELLAS BENÍTEZ AND CARLOS D'ANDREA

ABSTRACT. We compute a minimal bigraded free resolution of the Rees Algebra associated to a proper rational parametrization of a monomial plane curve. We describe explicitly the bigraded Betti numbers in terms of a generalized version of the Euclidean Algorithm.

The Rees algebra can be presented as the quotient of a polynomial ring by an ideal. This ideal is called the defining ideal of the Rees algebra and their generators are the defining equations of the Rees algebra. David Cox observed in [5] that this ideal is the moving curve ideal considered by the geometric modeling community. Partially motivated by this connection, in the last years a lot of attention has been given to compute the defining equations of Rees algebras of a parametrization, see for instance [6, 8, 1, 9, 11, 10, 2, 7, 3, 4, 12].

We deal with the case of a monomial plane curve

$$\begin{array}{cccc} \varphi: & \mathbb{P}^1_{\mathbb{K}} & \to & \mathbb{P}^2_{\mathbb{K}} \\ & (t_0:t_1) & \mapsto & \big(t_0^d : t_0^{d-u}t_1^u : t_1^d\big). \end{array}$$

where $\mathbb{P}^i_{\mathbb{K}}$, $i=1,2$, denotes the projective space of dimension i over a field $\mathbb{K}$ and $u,\, d$ are positive integers such that $u<\frac{d}{2}$ and $\gcd(u,d)=1$.

Denote with $\underline{T}$ the sequence of variables $T_0,\, T_1$, and set $\mathrm{R}=\mathbb{K}[\underline{T}]$. Consider the homogeneous ideal $\mathcal{I}=\langle T_0^d,\, T_0^{d-u}T_1^u,\, T_1^d\rangle\subset\mathrm{R}$. The *Rees Algebra* of φ is $\mathrm{Rees}(\mathcal{I})=\oplus_{n\geq 0}\mathcal{I}^nZ^n$, where Z is a new variable. Let $X_0,\, X_1,\, X_2$ be three other variables, and set $\underline{X}=X_0,\, X_1,\, X_2$. There is an epimorphism of R-algebras defined by

$$\begin{array}{cccc} \mathrm{S}:=\mathrm{R}[\underline{X}] & \overset{\Phi_0}{\to} & \mathrm{Rees}(\mathcal{I}) & \to\ 0 \\ X_0 & \mapsto & T_0^dZ & \\ X_1 & \mapsto & T_0^{d-u}T_1^uZ & \\ X_2 & \mapsto & T_1^dZ. & \end{array}$$

We consider $\mathrm{Rees}(\mathcal{I})$ as a finitely generated S-module via Φ_0. If we declare that $\mathrm{bideg}(Z)=(-d,1)$, $\mathrm{bideg}(T_i)=(1,0)$ and $\mathrm{bideg}(X_j)=(0,1)$ for $i=0,1,\ j=0,\,1,\,2$ then Φ_0 is a bihomogeneous (of bidegree $(0,0)$) S-linear map. The kernel of Φ_0 is the defining ideal of $\mathrm{Rees}(\mathcal{I})$. Our main result is an explicit description of a minimal bigraded free resolution of $\mathrm{Rees}(\mathcal{I})$. Indeed, if we do not keep track of the graduation, we can show that such a minimal resolution is of the form

$$0\to\mathrm{S}^{q-1}\to\mathrm{S}^{2q}\to\mathrm{S}^{q+2}\to\mathrm{S}\overset{\Phi_0}{\to}\mathrm{Rees}(\mathcal{I})\to 0,$$

for a suitable positive integer q.

To do this, for the data (d,u) we consider the standard *Euclidean Remainder Sequence* which is defined as follows: $a_0=d-u,\ a_1=u$. For $1\leq i\leq p-1$ we write $a_{i-1}=q_ia_i+a_{i+1}$, with

This is an extended abstract of the paper arXiv:1311.5488v1.

$q_i,\, a_{i+1} \in \mathbb{Z},\, 0 \leq a_{i+1} < a_i$. The number $p = p(d,u)$ is such that $a_p = 0$. The exponent q in the resolution is $q := \sum_{m=1}^{p-1} q_m$.

We show how our method works by performing it on the data $(d,u) = (10,3)$.

The ordinary Euclidean algorithm for $(10,3)$ *gives* $\{a_n\} = \{7,\, 3,\, 1,\, 0\}$, $\{q_m\} = \{2,\, 3\}$, *and so* $p = 3$, $q = 5$.

To precise the bidegrees of the resolution; that is, the bigraded Betti numbers, we consider the *Slow Euclidean Remainder Sequence* (SERS) associated to (d,u), which are pairs of nonegative integers $\{(b_n,\, c_n)\}_{n=1,\ldots,q+1}$ defined recursively as follows: $b_1 = d - u$, $c_1 = u$, and for $0 \leq n \leq q$, the set $\{b_{n+1},\, c_{n+1}\}$ is equal to $\{b_n - c_n,\, c_n\}$, sorted in such a way that $b_{n+1} \geq c_{n+1}$.

The SERS associated to $(10,3)$ *is* $(b_1,c_1) = (7,3)$,$(b_2,c_2) = (4,3)$, $(b_3,c_3) = (3,1)$, $(b_4,c_4) = (2,1)$, $(b_5,c_5) = (1,1)$, $(b_6,c_6) = (1,0)$.

The SERS can be regarded as a way of performing the standard Euclidean Remainder Sequence without making any divisions. For any $n = 1,\ldots,q+1$, there is a standard way of writing $\sigma_n u + \tau_n(d-u) = b_n$, with $\sigma_n,\, \tau_n \in \mathbb{Z}$, $|\sigma_n| < d-u$, $|\tau_n| < u$ in the same way one unravels the Euclidean Remainder sequence to produce Bézout identities associated to u and $d-u$.

For the data $(10,3)$, *we have* $(\sigma_1,\tau_1) = (0,1)$, $(\sigma_2,\tau_2) = (-1,1)$, $(\sigma_3,\tau_3) = (1,0)$, $(\sigma_4,\tau_4) = (3,-1)$, $(\sigma_5,\tau_5) = (5,-2)$, $(\sigma_6,\tau_6) = (-2,1)$.

For $\ell = 0,\, 1,\ldots,p-1$, set $m_\ell = 1 + \sum_{j=1}^{\ell} q_j$. Also, set $m_p := q+2$. Given $n \in \{1,\ldots,q\}$, we define $\ell(n)$ as the unique ℓ such that $m_{\ell-1} \leq n < m_\ell$.

$\{m_l\} = \{1,\, 3,\, 6,\, 7\}$ *for* $(10,3)$.

Our main result is the following:

Theorem 0.1. *The minimal bigraded free resolution of* $\mathrm{Rees}(\mathcal{I})$ *is:*

$$0 \to \oplus_{n=1}^{q-1}\mathrm{S}(-(b_n, |\sigma_n - \tau_n| + 2|\sigma_{m_{\ell(n)}} - \tau_{m_{\ell(n)}}|)) \to$$
$$\xrightarrow{\Phi_3} \oplus_{n=1}^{q}\mathrm{S}(-(b_n, |\sigma_n - \tau_n| + |\sigma_{m_{\ell(n)}} - \tau_{m_{\ell(n)}}|))^2 \xrightarrow{\Phi_2} \oplus_{n=1}^{q+2}\mathrm{S}(-(b_n, |\sigma_n - \tau_n|)) \xrightarrow{\Phi_1} \mathrm{S} \xrightarrow{\Phi_0} \mathrm{Rees}(\mathcal{I}) \to 0.$$

To explicit the above resolution, we start by setting, using the notation introduced, for $n = 1,\ldots,q+1$,

$$G_{n,b_n}(\underline{T},\underline{X}) = \begin{cases} T_0^{b_n} X_0^{-\sigma_n} X_2^{\tau_n} - T_1^{b_n} X_1^{\tau_n - \sigma_n} & \text{if} \quad \sigma_n \leq 0, \\ T_0^{b_n} X_1^{\sigma_n - \tau_n} - T_1^{b_n} X_0^{\sigma_n} X_2^{-\tau_n} & \text{if} \quad \sigma_n > 0. \end{cases}$$

We define also $b_{q+2} = 0$ and

$$G_{q+2,0}(\underline{T},\underline{X}) = \begin{cases} X_0^{d-u} X_2^{u} - X_1^{d} & \text{if} \quad \sigma_q > 0 \\ X_1^{d} - X_0^{d-u} X_2^{u} & \text{if} \quad \sigma_q < 0. \end{cases}$$

Set $\mathcal{G}_0 := \{G_{n,b_n}(\underline{T},\underline{X})\}_{n=1,\ldots,q+2}$.

The elements in $\mathcal{G}_0$ can be also computed recursively by starting with $T_0^{d-u}X_2 - T_1^{d-u}X_1$ and $T_0^{u}X_1 - T_1^{u}X_0$, two distinguished elements of $\ker(\Phi_0)$ identified with the basis $(0, -T_1^{d-u}, T_0^{d-u})$ and $(-T_1^{u}, T_0^{u}, 0)$ of the syzygy module $\mathrm{syz}(\mathcal{I}) \subset \mathrm{R}^3$.

Theorem 0.2. $\mathcal{G}_0$ *is a reduced Gröbner basis of* $\ker(\Phi_0)$ *with respect to a suitable lexicographic order* $\prec_l$, *and a minimal set of generators of this ideal.*

So, to continue with the resolution, we must consider $F_1 := \bigoplus_{n=1}^{q+2} \mathrm{S}(-(b_n, |\sigma_n - \tau_n|))$ the free bigraded module with basis $\mathbf{e}_1, \ldots, \mathbf{e}_{q+2}$ and $\mathrm{bideg}(\mathbf{e}_n) = \mathrm{bideg}(G_{n,b_n}(\underline{T}, \underline{X})) = = (b_n, |\sigma_n - \tau_n|)$. Then we define Φ_1, in the natural way, sending e_n to $G_{n,b_n}(\underline{T}, \underline{X})$.

For the data $(10, 3)$

$$\begin{aligned} \mathcal{G}_0 = \{ \quad & T_0^7 X_2 - T_1^7 X_1,\, T_0^4 X_0 X_2 - T_1^4 X_1^2,\, T_0^3 X_1 - T_1^3 X_0, T_0^2 X_1^4 - T_1^2 X_0^3 X_2, \\ & T_0 X_1^7 - T_1 X_0^5 X_2^2,\, T_0 X_0^2 X_2 - T_1 X_1^3,\, X_0^7 X_2^3 - X_1^{10} \} \textit{ and} \end{aligned}$$

$$F_1 = \mathrm{S}(-(0,10)) \oplus \mathrm{S}(-(1,3)) \oplus \mathrm{S}(-(1,7)) \oplus \mathrm{S}(-(2,4)) \oplus \mathrm{S}(-(3,1)) \oplus \mathrm{S}(-(4,2)) \oplus \mathrm{S}(-(7,1)).$$

For the second step, we will endow the free module S^{q+2} with a term ordering $\prec_{l,\mathcal{G}_0}$ depending on both $\mathcal{G}_0$ and the term order $\prec_l$ on S. We define

$$\rho(n) = \begin{cases} n+1 & \text{if} \quad n+1 < m_\ell \\ m_{\ell+1} & \text{if} \quad n+1 = m_\ell. \end{cases}$$

By computing all the $\mathbf{S}$-polynomials

$$\mathbf{S}\big(G_{n,b_n}(\underline{T}, \underline{X}), G_{m_{\ell(n)}, b_{m_{\ell(n)}}}(\underline{T}, \underline{X})\big),\ \mathbf{S}\big(G_{n,b_n}(\underline{T}, \underline{X}), G_{\rho(n), b_{\rho(n)}}(\underline{T}, \underline{X})\big)$$

we can extract a set o $2q$ elements in $\mathrm{syz}(\mathcal{G}_0) = \mathrm{syz}(\ker(\Phi_0)) = \ker(\Phi_1) \subset \mathrm{S}^{q+2}$

We denote by $\mathcal{G}_1 := \{\mathbf{s}_{n,m_{\ell(n)}},\, \mathbf{s}_{n,\rho(n)}\}_{n=1,\ldots,q-1} \cup \{\mathbf{s}_{q,q+1},\, \mathbf{s}_{q+1,q+2}\}$ this set of syzygies.

Theorem 0.3. *$\mathcal{G}_1$ is a reduced Gröbner basis of* $\ker(\Phi_1)$ *with respect to $\prec_{l,\mathcal{G}_0}$, and a minimal set of generators of this module.*

This lead us to consider $F_2 := \bigoplus_{n=1}^{q} \mathrm{S}(-(b_n, |\sigma_n - \tau_n| + |\sigma_{m_{\ell(n)}} - \tau_{m_{\ell(n)}}|))^2$, with canonical basis $\{\mathbf{e}_{n,\rho(n)},\, \mathbf{e}_{n,m_{\ell(n)}}\}_{n=1,\ldots,q-1} \cup \{\mathbf{e}_{q,q+1} \mathbf{e}_{q+1,q+2}\}$, and declaring that

$$\begin{aligned} &\mathrm{bideg}(\mathbf{e}_{n,\rho(n)}) = \mathrm{bideg}(\mathbf{e}_{n,m_{\ell(n)}}) = \mathrm{bideg}(\mathbf{s}_{n,m_{\ell(n)}}) = \mathrm{bideg}(\mathbf{s}_{n,\rho(n)}) = (b_n, |\sigma_n - \tau_n| + |\sigma_{m_{\ell(n)}} - \tau_{m_{\ell(n)}}|), \\ &\mathrm{bideg}(\mathbf{e}_{q,q+1}) = \mathrm{bideg}(\mathbf{e}_{q+1,q+2}) = \mathrm{bideg}(\mathbf{s}_{q,q+1}) = \mathrm{bideg}(\mathbf{s}_{q,q+2}) = (1, d). \end{aligned}$$

The map Φ_2 is defined sending $\mathbf{e}_{n,k}$ to $\mathbf{s}_{n,k}$.

For the data $(10, 3)$*, $\mathcal{G}_1$ is the set of elements*

$$\begin{aligned} \mathbf{s}_{1,2} &= X_0 \mathbf{e}_1 - T_0^3 \mathbf{e}_2 - T_1^4 X_1 \mathbf{e}_3, & \mathbf{s}_{1,3} &= X_1 \mathbf{e}_1 - T_0^4 X_2 \mathbf{e}_3 - T_1^3 \mathbf{e}_2, \\ \mathbf{s}_{2,3} &= X_1 \mathbf{e}_2 - T_0 X_0 X_2 \mathbf{e}_3 - T_1^3 \mathbf{e}_6, & \mathbf{s}_{2,6} &= X_0 \mathbf{e}_2 - T_0^3 \mathbf{e}_6 - T_1 X_1^2 \mathbf{e}_3, \\ \mathbf{s}_{3,4} &= X_1^3 \mathbf{e}_3 - T_0 \mathbf{e}_4 - T_1^2 X_0 \mathbf{e}_6, & \mathbf{s}_{3,6} &= X_0^2 X_2 \mathbf{e}_3 - T_0^2 X_1 \mathbf{e}_6 - T_1 \mathbf{e}_4, \\ \mathbf{s}_{4,5} &= X_1^3 \mathbf{e}_4 - T_0 \mathbf{e}_5 - T_1 X_0^3 X_2 \mathbf{e}_6 & \mathbf{s}_{4,6} &= X_0^2 X_2 \mathbf{e}_4 - T_0 X_1^4 \mathbf{e}_6 - T_1 \mathbf{e}_5 \\ \mathbf{s}_{5,6} &= X_0^2 X_2 \mathbf{e}_5 - X_1^7 \mathbf{e}_6 + T_1 \mathbf{e}_7 & \mathbf{s}_{6,7} &= X_0^5 X_2^2 \mathbf{e}_6 - T_0 \mathbf{e}_7 + X_1^3 \mathbf{e}_5. \end{aligned}$$

and one has

$$F_2 = \mathrm{S}(-(1,10))^2 \oplus \mathrm{S}(-(2,7))^2 \oplus \mathrm{S}(-(3,4))^2 \oplus \mathrm{S}(-(4,3))^2 \oplus \mathrm{S}(-(7,2))^2.$$

To complete our description we consider S^{2q} with the induced order $\prec_{l,\mathcal{G}_1}$, and we also make explicit a set of $q-1$ elements $\mathcal{G}_2 := \{\mathbf{s}_{n,\rho(n),\ell(n)}\}_{n=1,\ldots,q-1}$ in $\mathrm{syz}(\mathcal{G}_1) \subset \mathrm{S}^{2q}$.

Theorem 0.4. *$\mathcal{G}_2$ is a Gröbner basis of* $\ker(\Phi_2)$ *with respect to $\prec_{l,\mathcal{G}_1}$. This set is also* S*-linearly independent. In particular* $\ker(\Phi_2)$ *is a free* S*-module with basis $\mathcal{G}_2$.*

Thus, if $F_3 := \bigoplus_{n=1}^{q-1} \mathrm{S}(-(b_n, |\sigma_n - \tau_n| + 2|\sigma_{m_{\ell(n)}} - \tau_{m_{\ell(n)}}|))$ with basis $\{\mathbf{e}_{n,\rho(n),\ell(n)}\}_{n=1,\ldots,q-1}$, having bidegrees $\mathrm{bideg}(\mathbf{e}_{(n,\rho(n),\ell(n))}) = (b_n, |\sigma_n - \tau_n| + 2|\sigma_{m_{\ell(n)}} - \tau_{m_{\ell(n)}}|)$, Φ_3 sends $\mathbf{e}_{n,\rho(n),\ell(n)}$ to $\mathbf{s}_{n,\rho(n),\ell(n)}$.

For the data $(10, 3)$*,* $\mathcal{G}_2$ *is made by the syzygies*

$$\mathbf{s}_{1,2,3} = X_1\mathbf{e}_{1,2} - X_0\mathbf{e}_{1,3} + T_0^3\mathbf{e}_{2,3} - T_1^3\mathbf{e}_{2,6}, \qquad \mathbf{s}_{2,3,6} = X_0\mathbf{e}_{2,3} - X_1\mathbf{e}_{2,6} + T_0\mathbf{e}_{3,6} - T_1\mathbf{e}_{3,4},$$
$$\mathbf{s}_{3,6,3} = X_0^2X_2\mathbf{e}_{3,4} - X_1^3\mathbf{e}_{3,6} + T_0\mathbf{e}_{4,6} - T_1\mathbf{e}_{4,5}, \quad \mathbf{s}_{4,5,6} = X_0^2X_2\mathbf{e}_{4,5} - X_1^3\mathbf{e}_{4,6} + T_0\mathbf{e}_{5,6} - T_1\mathbf{e}_{5,7}.$$

and $F_3 = \mathrm{S}(-(2, 10)) \oplus \mathrm{S}(-(3, 7)) \oplus \mathrm{S}(-(4, 4)) \oplus \mathrm{S}(-(7, 3))$.

REFERENCES

[1] Busé, Laurent. *On the equations of the moving curve ideal of a rational algebraic plane curve.* J. Algebra 321 (2009), no. 8, 2317–2344.

[2] Cortadellas Benítez, Teresa; D'Andrea, Carlos. *Minimal generators of the defining ideal of the Rees Algebra associated to monoid parametrizations.* Computer Aided Geometric Design, Volume 27, Issue 6, August 2010, 461–473.

[3] Cortadellas Benítez, Teresa; D'Andrea, Carlos. *Rational plane curves parametrizable by conics.* J. Algebra 373 (2013) 453–480.

[4] Cortadellas Benítez, Teresa; D'Andrea, Carlos. *Minimal generators of the defining ideal of the Rees Algebra associated to a rational plane parameterization with* $\mu = 2$. To appear in *Canadian Journal of Mathematics.*

[5] Cox, David A. *The moving curve ideal and the Rees algebra.* Theoret. Comput. Sci. 392 (2008), no. 1-3, 23–36.

[6] Cox, David; Hoffman, J. William; Wang, Haohao. *Syzygies and the Rees algebra.* J. Pure Appl. Algebra 212 (2008), no. 7, 1787–1796.

[7] Hassanzadeh, Seyed Hamid; Simis, Aron. *Implicitization of the Jonquières parametrizations.* To appear in J. Commut. Algebra.

[8] Hong, Jooyoun; Simis, Aron; Vasconcelos, Wolmer V. *On the homology of two-dimensional elimination.* J. Symbolic Comput. 43 (2008), no. 4, 275–292.

[9] Hong, Jooyoun; Simis, Aron; Vasconcelos, Wolmer V. *Equations of almost complete intersections.* Bulletin of the Brazilian Mathematical Society, June 2012, Volume 43, Issue 2, 171–199.

[10] Hoffman, J. William; Wang, Haohao. *Defining equations of the Rees algebra of certain parametric surfaces.* Journal of Algebra and its Applications, Volume: 9, Issue: 6(2010), 1033–1049

[11] Kustin, Andrew R.; Polini, Claudia; Ulrich, Bernd. *Rational normal scrolls and the defining equations of Rees Algebras.* J. Reine Angew. Math. 650 (2011), 23–65.

[12] Kustin, Andrew; Polini, Claudia; Ulrich, Bernd. *The bi-graded structure of Symmetric Algebras with applications to Rees rings.* arXiv:1301.7106 .

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

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

NULL SPACE OF THE BEZOUT MATRIX AND GCD'S

GEMA MARÍA DÍAZ-TOCA AND MARIO FIORAVANTI

ABSTRACT. The aim of this talk is to present new results on the structure of the null space of the Bezout matrix of two polynomials, and a new method for computing the gcd of several polynomials from the null space of Bezout matrices. The main point is that the presented results are expressed with respect to a general (arbitrary) polynomial basis. In recent years, many problems in polynomial systems, stability theory, CAGD, etc., have been solved using Bezout matrices in distinct specific bases. Therefore, it is very useful to have results and tools that can be applied to any basis.

1. DEFINITION OF THE BEZOUT MATRIX

The classical definition of the Bezout matrix makes explicit reference to the monomial basis, and it can be found, together with its main properties, in the books [3], [5], [6], [8] and [9], or in the article [7]. Nevertheless, the definition of the Bezout matrix makes use of the so-called Cayley quotient, which makes no reference to any particular basis in which the given polynomials are represented. Indeed, in [1, 10] one can find the following definition.

Definition 1.1. Let $P(t), Q(t)$ be two polynomials in $\mathbb{K}[t]$, where $\mathbb{K}$ is a field of characteristic zero, usually $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$, and $n = \max\{\deg(P(t)), \deg(Q(t))\}$. The Cayley quotient of $P(t)$ and $Q(t)$ is the polynomial $C_{P,Q}$ defined by

$$C_{P,Q}(t,x) = \frac{P(t)Q(x) - P(x)Q(t)}{t-x} \tag{1}$$

Thus, if $\mathbf{\Phi}(t) = \{\phi_0(t), \ldots, \phi_{n-1}(t)\}$ is a basis of the vector space of polynomials of degree at most $n-1$, denoted by $\mathbb{P}_{n-1}$, then $C_{P,Q}$ can be written as

$$C_{P,Q}(t,x) = \sum_{i,j=0}^{n-1} b_{ij}\phi_i(t)\phi_j(x) = (\phi_0(t), \ldots, \phi_{n-1}(t))\,(b_{ij}) \begin{pmatrix} \phi_0(x) \\ \vdots \\ \phi_{n-1}(x) \end{pmatrix}. \tag{2}$$

The symmetric matrix $\mathbf{Bez}_{\mathbf{\Phi}}(P,Q) = (b_{ij}) \in M_n(\mathbb{K})$ is called the Bezout matrix in the basis $\mathbf{\Phi}(t)$.

Obviously, Bezout matrices associated to different basis are congruent. Given two distinct basis of $\mathbb{P}_{n-1}$, $\mathbf{\Phi}(t)$ and $\mathbf{\Psi}(t)$, and the transformation matrix $\mathbf{P}_{\Psi\to\Phi}$ between $\mathbf{\Psi}(t)$ and $\mathbf{\Phi}(t)$ such that

$$(\phi_0(t), \ldots, \phi_{n-1}(t))\,\mathbf{P}_{\Psi\to\Phi} = (\psi_0(t), \ldots, \psi_{n-1}(t)),$$

then

$$\mathbf{Bez}_{\Phi}(P,Q) = \mathbf{P}_{\Psi\to\Phi}\mathbf{Bez}_{\Psi}(P,Q)\mathbf{P}^T_{\Psi\to\Phi}.$$

2. THE NULL SPACE OF THE BEZOUT MATRIX

2.1. **The null space of $\mathbf{Bez}_{\mathrm{St}}(\mathbf{P},\mathbf{Q})$.** Let $\mathrm{St} = \{1, t, \ldots, t^{n-1}\}$ denote the monomial basis of $\mathbb{P}_{n-1}$. In [6], G. Heinig and K. Rost describe the structure of the null space of the Bezout matrix in the monomial basis (for a proof see [6], page 42).

Theorem 2.1. *The null space of* $\mathbf{Bez}_{\mathrm{St}}(P,Q)$ *is spanned by the columns of the matrix* $(X_1, X_2, \ldots, X_k)$ *where each block* X_j *corresponds to a different common root of* $P(t)$ *and* $Q(t)$ *and its dimension is the geometric multiplicity* k_j *of the common root* x_j *(i.e., its multiplicity as a root of the greatest common divisor of* $P(t)$ *and* $Q(t)$*). Moreover each block can be parameterized by the common root* x_j *in the form*

$$X_j = \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 \\ x_j & 1 & 0 & \ldots & 0 \\ x_j^2 & 2x_j & 2 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ x_j^{n-1} & (n-1)x_j^{n-2} & (n-1)(n-2)x_j^{n-3} & \ldots & (n-1)^{\underline{k_j-1}} x_j^{n-k_j} \end{pmatrix} \tag{3}$$

where $n^{\underline{k_j}} = n(n-1)\cdots(n-k_j+1)$.

In particular, if the null space is spanned by $(1, \alpha, \ldots, \alpha^{n-1})$, with α the unique common root of $P(t)$ and $Q(t)$ and if $(v_1, \ldots, v_n)$ is a nonzero vector of the null space, then $\alpha = \frac{v_2}{v_1}$.

2.2. **The null space of $\mathbf{Bez}_{\mathbf{\Phi}}(\mathbf{P},\mathbf{Q})$.** To generalize Theorem 2.1, it is convenient to previously state the following natural result.

Lemma 2.2. *Let* $i \le n-1$ *and let* $\phi_j^{(i)}(t)$ *denote the i-th derivative of the polynomial* $\phi_j(t)$ *for* $j \le n-1$. *Then,*

$$\mathbf{P}^T_{\Phi\to\mathrm{St}} \begin{pmatrix} 0 \\ \vdots \\ 0 \\ i! \\ \vdots \\ (n-1)^{\underline{i}}\, t^{n-1-i} \end{pmatrix} = \begin{pmatrix} \phi_1^{(i)}(t) \\ \vdots \\ \vdots \\ \vdots \\ \phi_n^{(i)}(t) \end{pmatrix}$$

For a proof, see [4]. Then, the following generalization of Theorem 2.1 can be infered (see [4]).

Theorem 2.3. *The null space of* $\mathbf{Bez}_{\Phi}(P,Q)$ *is spanned by the columns of the matrix* $\left(X_1^{\Phi}, X_2^{\Phi}, \ldots, X_k^{\Phi}\right)$, *where each block* X_j^{Φ} *corresponds to a different common root of* $P(t)$ *and* $Q(t)$ *and its dimension is the geometric multiplicity,* k_j, *of the common root* x_j. *This block is given by*

$$X_j^{\Phi} = \begin{pmatrix} \phi_1(x_j) & \phi_1^{(1)}(x_j) & \ldots & \phi_1^{(k_j-1)}(x_j) \\ \phi_2(x_j) & \phi_2^{(1)}(x_j) & \ldots & \phi_2^{(k_j-1)}(x_j) \\ \vdots & \vdots & & \vdots \\ \phi_{n-1}(x_j) & \phi_{n-1}^{(1)}(x_j) & \ldots & \phi_{n-1}^{(k_j-1)}(x_j) \end{pmatrix} \tag{4}$$

Finally, the next result provides a closed expression for α if it is the only common root, and it has multiplicity equal to one.

Proposition 2.4. *Let $P(t)$ and $Q(t)$ be univariate polynomials with only one simple common root α. Let $1 = a_1\phi_0(t) + \ldots + a_n\phi_{n-1}(t)$, and $t = b_1\phi_0(t) + \ldots + b_n\phi_{n-1}(t)$. If $(u_1, u_2, \ldots, u_n)^T$ is a non zero vector in the null space of $\mathbf{Bez}_\Phi(P, Q)$, then*

$$\alpha = \frac{b_1u_1 + \ldots + b_nu_n}{a_1u_1 + \ldots + a_nu_n}. \tag{5}$$

For a proof, see [4].

Example 2.5. We consider Example 3 from [2]. Let $P(t)$ and $Q(t)$ in $\mathbb{P}_4$ be expressed in the Bernstein basis $\beta = \{\beta_i^{(4)}(t) = \binom{4}{i}(1-t)^{4-i}t^i, 0 \leq i \leq 4\}$ as follows

$$P(t) = 4\beta_0^{(4)}(t) + 4\beta_1^{(4)}(t) + \frac{19}{6}\beta_2^{(4)}(t) + \frac{3}{2}\beta_3^{(4)}(t),$$

$$Q(t) = \frac{1}{2}\beta_0^{(4)}(t) + \frac{7}{16}\beta_1^{(4)}(t) + \frac{1}{24}\beta_2^{(4)}(t) - \frac{7}{16}\beta_3^{(4)}(t) - \frac{3}{4}\beta_4^{(4)}(t).$$

Then, the Bezout matrix in the Bernstein basis is equal to

$$\mathbf{Bez}_\beta(P, Q) = \begin{bmatrix} 1 & \frac{17}{6} & \frac{10}{3} & 3 \\ \frac{17}{6} & \frac{157}{36} & \frac{83}{18} & 4 \\ \frac{10}{3} & \frac{83}{18} & \frac{187}{36} & \frac{19}{4} \\ 3 & 4 & \frac{19}{4} & \frac{9}{2} \end{bmatrix},$$

and its null space is spanned by the vector $(-1, 6, -12, 8)$. Thus, they have only one simple common root. Moreover, since $1 = \sum\limits_{k=0}^{3} \beta_k^{(3)}(t)$ and $t = \sum\limits_{k=1}^{3} \frac{k}{3}\beta_k^{(3)}(t)$, then, by Proposition 2.4, their common root is equal to 2:

$$2 = \frac{\frac{1}{3}6 - \frac{2}{3}12 + 8}{(-1 + 6 - 12 + 8)}.$$

3. Null spaces and gcd's

Let

$$\mathbf{B}_{\mathrm{St}}^P(Q_1, \ldots, Q_r) = \begin{pmatrix} \mathbf{Bez}_{\mathrm{St}}(P, Q_1) \\ \vdots \\ \mathbf{Bez}_{\mathrm{St}}(P, Q_r) \end{pmatrix},$$

where $\deg(P(t)) = n$ and $\deg(Q_i(t)) \leq n$ for $1 \leq r$. The following result shows how to compute the coefficients of the greatest common divisor of $P(t), Q_1(t), \ldots, Q_r(t)$, from the null space of the matrix $\mathbf{B}_{\mathrm{St}}^P(Q_1, \ldots, Q_r)$. The method is justified first in the monomial basis, and then it is generalized to an arbitrary basis.

Proposition 3.1. *Suppose* $\gcd(P, Q_1, \ldots, Q_r) = t^k + d_1t^{k-1} + \ldots + d_k$. *Let $\mathbf{N} \in \mathcal{M}_{n\times k}(\mathbb{K})$ be a matrix whose set of columns forms a basis of the* $\mathrm{nullspace}(\mathbf{B}_{\mathrm{St}}^P(Q_1, \ldots, Q_r))$, *and let $\mathbf{Z}$ be the submatrix of $\mathbf{N}$ defined by the first $k + 1$ rows. Then we have*

$$(d_k, \ldots, d_1, 1)\,\mathbf{Z} = (0, \ldots, 0). \tag{6}$$

For a proof, see [4]. Hence, the greatest common divisor for several polynomials can be computed by solving the linear system (6). The generalization of this result is as follows.

Corollary 3.2. *Let* $\mathbf{N}^{\Phi} \in \mathcal{M}_{n\times k}(\mathbb{K})$ *be a matrix whose columns define a basis of the* $\mathrm{nullspace}(\mathbf{Bez}_{\Phi}^{P}(Q_1,\ldots,Q_r))$ *Thus, if* $\mathbf{Z}^{\boldsymbol{\Phi}}$ *denotes the matrix defined by the first* $k+1$ *rows of* $\mathbf{P}_{\mathrm{St}\to\Phi}^{T}\mathbf{N}^{\boldsymbol{\Phi}}$*, then*

$$(d_k,\ldots,d_1,1)\,\mathbf{Z}^{\boldsymbol{\Phi}} = (0,\ldots,0).$$

4. Acknowledgments

The authors are partially supported by the Spanish “Ministerio de Economía y Competitividad" and by the European Regional Development Fund (ERDF), under the Project MTM2011-25816-C02-02. Moreover, we wish to thank the anonymous referees whose valuable suggestions greatly improved the presentation of the paper.

References

[1] S. Basu and R. Pollack and M.F. Roy. *Algorithms in real algebraic geometry, 2nd edition.* Springer Verlag, Berlin, 2006.

[2] D. A. Bini and L. Gemignani. *Bernstein-Bezoutian matrices.* Theoretical Computer Science 315, 319–333, 2004.

[3] Dario Bini and Victor Pan. *Polynomial and Matrix Computations.* Birkhäuser, 1994.

[4] M. Fioravanti and G.M. Diaz–Toca. *The null space of the Bezout matrix in any basis and gcd's.* Preprint, 2014.

[5] P.A. Fuhrmann. *A Polynomial Approach to Linear Algebra.* Springer Verlag, New York, 1996.

[6] Georg Heinig and Karla Rost. *Algebraic methods for Toeplitz-like matrices and operators.* Birkhaüser, 1984.

[7] U. Helmke and P.A. Fuhrmann. *Bezoutians.* Linear Algebra and Its Applications 122/123/124,1039–1097, 1989

[8] P. Lancaster and M. Tismenetsky. *The theory of matrices.* Computer Science and Applied Mathematics. Academic Press, 1985

[9] M. Mignotte. *Mathematics for Computer Algebra*, Springer Verlag, New York, 1992

[10] Zheng-Hong Yang. *Polynomial Bezoutian matrix with respect to a general basis.* Linear Algebra and Its Applications 331, 165–179, 2001.

Departamento de Matemática Aplicada, Universidad de Murcia, Spain
E-mail address: gemadiaz@um.es

Departamento de Matemáticas, Estadística y Computación, Universidad de Cantabria, Spain.
E-mail address: mario.fioravanti@unican.es

SIGNATURE-BASED GRÖBNER BASIS ALGORITHMS IN SINGULAR

CHRISTIAN EDER

ABSTRACT. In 2001 Faugère published his **F5** algorithm for computing Gröbner bases. This algorithm is known to compute no zero reductions for regular input sequences and it has broken several previously untractable problems, for example in cryptanalysis. Using signatures **F5** can detect useless computations in advance. Over the years many variants of this algorithm have been published with slight optimizations. Version $4-0-0$ of SINGULAR provides the first open-source implementation of signature-based Gröbner basis algorithms including all variants known.

1. INTRODUCTION

Since 1965 [2] Gröbner bases are practically feasible. One of the main algorithmic improvements is the prediction of useless data during the computations. That means to use criteria to detect zero reductions in advance [3, 4]. Gebauer and Möller gave an optimal implementation of Buchberger's criteria [12], but showed that not all zero reductions are discarded. In 2002 Faugère presented the **F5** algorithm [9] which uses new criteria based on so-called "signatures". For regular input sequences **F5** does not compute any zero reduction at all. Thus a new class of so-called "signature-based" Gröbner basis algorithms emerged, see, for example, [1, 6, 7, 11, 13].

We present a basic version we call **SBA** with which we explain the ideas behind this kind of algorithms easily. Moreover, we present experimental results for an efficient implementation in the computer algebra system SINGULAR [5] that is open-source and includes all known variants.

2. NOTATIONS

Let $\mathcal{R}$ be a polynomial ring over a field $\mathcal{K}$. All polynomials $f \in \mathcal{R}$ can be uniquely written as a finite sum $f = \sum_{\kappa_v x^v \in \mathcal{M}} \kappa_v x^v$ where $\kappa_v \in \mathcal{K}$, $x^v := \prod_i x_i^{v_i}$ and $\mathcal{M}$ is minimal. The elements of $\mathcal{M}$ are the *terms* of f. A *monomial* is a polynomial with exactly one term. A monomial with a coefficient of 1 is *monic*. $f \simeq g$ for $f, g \in \mathcal{R}$ if there exists a non-zero $\kappa \in \mathcal{K}$ such that $f = \kappa g$.

Let $\mathcal{R}^m$ be a free $\mathcal{R}$-module and let $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_m$ be the canonical basis of unit vectors in $\mathcal{R}^m$. $\alpha \in \mathcal{R}^m$ can be uniquely written as a finite sum $\alpha = \sum_{a\boldsymbol{e}_i \in \mathcal{N}} a\boldsymbol{e}_i$ where the a are monomials and $\mathcal{N}$ is minimal. The elements of $\mathcal{N}$ are the *terms* of α. A *module monomial* is an element of $\mathcal{R}^m$ with exactly one term. A module monomial with a coefficient of 1 is *monic*. Let $\alpha \simeq \beta$ for $\alpha, \beta \in \mathcal{R}^m$ if $\alpha = \kappa\beta$ for some non-zero $\kappa \in \mathcal{K}$.

Consider a finite sequence of polynomials $f_1, \ldots, f_m \in \mathcal{R}$. We call $f_1, \ldots, f_m$ a regular sequence if f_i is a non-zero-divisor on $\mathcal{R}/\langle f_1, \ldots, f_{i-1}\rangle$ for $i = 2, \ldots, m$. We define the homomorphism $\alpha \mapsto \overline{\alpha}$ from $\mathcal{R}^m$ to $\mathcal{R}$ by $\overline{\alpha} := \sum_{i=1}^m \alpha_i f_i$. An element $\alpha \in \mathcal{R}^m$ with $\overline{\alpha} = 0$ is called a *syzygy*. The module of all syzygies of $f_1, \ldots, f_m$ is denoted by $\operatorname{syz}(f_1, \ldots, f_m)$.

Let $\leq$ denote two different orders – one for $\mathcal{R}$ and one for $\mathcal{R}^m$: The order for $\mathcal{R}$ is a monomial order, which means that it is a well-order on the set of monomials in $\mathcal{R}$ such that $a \leq b$ implies $ca \leq cb$ for all monomials $a, b, c \in \mathcal{R}$. The order for $\mathcal{R}^m$ is a module monomial order which means that it is a well-order on the set of module monomials in $\mathcal{R}^m$ such that $S \leq T$ implies $cS \leq cT$ for all module monomials $S, T \in \mathcal{R}^m$ and monomials $c \in \mathcal{R}$. We require the two orders to be *compatible* in the sense that $a \leq b$ if and only if $a\boldsymbol{e}_i \leq b\boldsymbol{e}_i$ for all monomials $a, b \in \mathcal{R}$ and $i = 1, \ldots, m$. The following compatible orders are commonly used in signature-based Gröbner basis algorithms.

Definition 1. *Let $<$ be a monomial order on $\mathcal{R}$ and let ae_i, be_j be two module monomials in $\mathcal{R}^m$. $ae_i <_{\text{pot}} be_j$ iff $i < j$ or $i = j$ and $a < b$. This can be combined by either a weighted degree or a weighted leading monomial:*

(a) $ae_i <_{\text{d-pot}} be_j$ iff $\deg\left(\overline{ae_i}\right) < \deg\left(\overline{be_j}\right)$ or $\deg\left(\overline{ae_i}\right) = \deg\left(\overline{be_j}\right)$ and $a\boldsymbol{e}_i <_{\text{pot}} b\boldsymbol{e}_j$.

(b) $ae_i <_{\text{lt-pot}} be_j$ iff $\operatorname{lt}\left(\overline{ae_i}\right) < \operatorname{lt}\left(\overline{be_j}\right)$ or $\operatorname{lt}\left(\overline{ae_i}\right) = \operatorname{lt}\left(\overline{be_j}\right)$ and $a\boldsymbol{e}_i <_{\text{pot}} b\boldsymbol{e}_j$.

Definition 2.

(a) The lead term *resp.* signature $\mathfrak{s}(\alpha)$ *of $\alpha \in \mathcal{R}^m \setminus \{0\}$ denotes the $\leq$-maximal term of α. If $a\boldsymbol{e}_i = \mathfrak{s}(\alpha)$ then we call* $\operatorname{ind}(\alpha) := i$ *the* index *of α. For $\overline{\alpha} \in \mathcal{R} \setminus \{0\}$ the* lead term $\operatorname{lt}(\overline{\alpha})$ *is the $\leq$-maximal term of f. The* lead coefficient $\operatorname{lc}(\overline{\alpha})$ *is the coefficient of* $\operatorname{lt}(\overline{\alpha})$.

(b) For $\alpha \in \mathcal{R}^m$ the sig-poly pair *of α is $(\mathfrak{s}(\alpha), \overline{\alpha}) \in \mathcal{R}^m \times \mathcal{R}$. $\alpha, \beta \in \mathcal{R}^m$ are* equal up to sig-poly pairs *if $\mathfrak{s}(\alpha) = \mathfrak{s}(\kappa\beta)$ and $\overline{\alpha} = \overline{\kappa\beta}$ for some non-zero $\kappa \in \mathcal{K}$. Correspondingly, α, β are said to be* equal up to sig-lead pairs *if $\mathfrak{s}(\alpha) = \mathfrak{s}(\kappa\beta)$ and $\operatorname{lt}(\overline{\alpha}) = \operatorname{lt}\left(\overline{\kappa\beta}\right)$ for some non-zero $\kappa \in \mathcal{K}$.*

3. Signature Gröbner bases

Every non-syzygy module element $\alpha \in \mathcal{R}^m$ has two main associated characteristics – the signature $\mathfrak{s}(\alpha) \in \mathcal{R}^m$ and the polynomial lead term $\operatorname{lt}(\overline{\alpha}) \in \mathcal{R}$. Lead terms and signatures include a coefficient for mathematical convenience, an implementation of a signature-based Gröbner basis algorithm over fields need not store the signature coefficients. To keep track of the signatures we get a classic polynomial reduction together with a further condition.

Definition 3. *Let $\alpha \in \mathcal{R}^m$ and let t be a term of $\overline{\alpha}$. Then we can* $\mathfrak{s}$-reduce *t by $\beta \in \mathcal{R}^m$ if there exists a monomial b such that* $\operatorname{lt}\left(\overline{b\beta}\right) = t$ *and $\mathfrak{s}(b\beta) \leq \mathfrak{s}(\alpha)$.*

The outcome of the $\mathfrak{s}$-reduction step is then $\alpha - b\beta$ and β is called the *$\mathfrak{s}$-reducer*. When β $\mathfrak{s}$-reduces t we also say for convenience that $b\beta$ $\mathfrak{s}$-reduces α. That way b is introduced implicitly instead of repeating the equation $\operatorname{lt}\left(\overline{b\beta}\right) = t$. Just as for classic polynomial reduction, if $\operatorname{lt}\left(\overline{b\beta}\right) \simeq \operatorname{lt}(\overline{\alpha})$ then the $\mathfrak{s}$-reduction step is a *top $\mathfrak{s}$-reduction step* and otherwise it is a *tail $\mathfrak{s}$-reduction step*. Analogously we define the distinction for signatures: If $\mathfrak{s}(b\beta) \simeq \mathfrak{s}(\alpha)$ then the reduction step is a *singular $\mathfrak{s}$-reduction step* and otherwise it is a *regular $\mathfrak{s}$-reduction step*. The result of an $\mathfrak{s}$-reduction of $\alpha \in \mathcal{R}^m$ is $\gamma \in \mathcal{R}^m$ that has been calculated from α through a sequence of $\mathfrak{s}$-reduction steps such that γ cannot be further $\mathfrak{s}$-reduced. The reduction is a *tail $\mathfrak{s}$-reduction* if only tail $\mathfrak{s}$-reduction steps are allowed and it is a *top $\mathfrak{s}$-reduction* if only top $\mathfrak{s}$-reduction steps are allowed. The reduction is a *regular $\mathfrak{s}$-reduction* if only regular $\mathfrak{s}$-reduction steps are allowed. $\alpha \in \mathcal{R}^m$ is *$\mathfrak{s}$-reducible* if it can be $\mathfrak{s}$-reduced. If α $\mathfrak{s}$-reduces to γ and γ is a syzygy then we say that α *$\mathfrak{s}$-reduces to zero* even if $\gamma \neq 0$. Note that analogously to the classic polynomial reduction $\mathfrak{s}$-reduction is always with respect to a finite *basis* $\mathcal{G} \subset \mathcal{R}^m$. The $\mathfrak{s}$-reducers in $\mathfrak{s}$-reduction are chosen from the basis $\mathcal{G}$.

Definition 4. *Let I be an ideal in $\mathcal{R}$. A finite subset $\mathcal{G} \subset \mathcal{R}^m$ is a* signature Gröbner basis in signature *T (for I) if all $\alpha \in \mathcal{R}^m$ with $\mathfrak{s}(\alpha) = T$ $\mathfrak{s}$-reduce to zero w.r.t. $\mathcal{G}$. $\mathcal{G}$ is a* signature Gröbner basis up to signature *T (for I) if $\mathcal{G}$ is a signature Gröbner basis in all signatures S such that $S < T$. $\mathcal{G}$ is a* signature Gröbner basis *(for I) if it is a signature Gröbner basis for I in all signatures. We denote $\overline{\mathcal{G}} := \{\overline{\alpha} \mid \alpha \in \mathcal{G}\} \subset \mathcal{R}$.*

Lemma 5 ([13])**.** *If $\mathcal{G}$ is a signature Gröbner basis then $\overline{\mathcal{G}}$ is a Gröbner basis.*

Next we give an algorithmic description of signature Gröbner bases.

Definition 6. *Let $\alpha, \beta \in \mathcal{R}^m$ such that $\overline{\alpha} \neq 0$, $\overline{\beta} \neq 0$ and let the monic least common multiple of* $\operatorname{lt}(\overline{\alpha})$ *and* $\operatorname{lt}(\overline{\beta})$ *be* $\lambda = \operatorname{lcm}\left(\operatorname{lt}(\overline{\alpha}), \operatorname{lt}(\overline{\beta})\right)$. *The* S-pair *between α and β is given by* $\operatorname{spair}(\alpha, \beta) := \frac{\lambda}{\operatorname{lt}(\overline{\alpha})}\alpha - \frac{\lambda}{\operatorname{lt}(\overline{\beta})}\beta$. $\operatorname{spair}(\alpha, \beta)$ *is* singular *if* $\mathfrak{s}\left(\frac{\lambda}{\operatorname{lt}(\overline{\alpha})}\alpha\right) \simeq \mathfrak{s}\left(\frac{\lambda}{\operatorname{lt}(\overline{\beta})}\beta\right)$. *Otherwise it is* regular.

Theorem 7 ([14])**.** *Let T be a module monomial of $\mathcal{R}^m$ and let $\mathcal{G} \subset \mathcal{R}^m$ be a finite basis. Assume that all regular S-pairs* $\operatorname{spair}(\alpha, \beta)$ *with $\alpha, \beta \in \mathcal{G}$ and* $\mathfrak{s}(\operatorname{spair}(\alpha, \beta)) < T$ *$\mathfrak{s}$-reduce to zero and all $\boldsymbol{e}_i$ with $\boldsymbol{e}_i < T$ $\mathfrak{s}$-reduce to zero. Then $\mathcal{G}$ is a signature Gröbner basis up to signature T.*

Note the similarity of Theorem 7 and Buchberger's criterion [2]. Theorem 7 suggests to consider only regular S-pairs for the computation of signature Gröbner bases. Thus in the following "S-pair" always refers to "regular S-pair".

4. A SIGNATURE-BASED GRÖBNER BASIS ALGORITHM

SBA is a generic signature-based algorithm in the vein of Buchberger's algorithm. Its efficiency depends on Line 7 that implements the Rewritten criterion (Lemma 8) to predict zero reductions.

The main differences to Buchberger's algorithm are the regular $\mathfrak{s}$-reduction in Line 8 and the set $\mathcal{H}$ which consists of found syzygies during the computation. Those syzygies are then used to remove useless elements in **Rewritable**. Moreover, **UpdateSyz** describes a generic subalgorithm that updates $\mathcal{H}$ and tries to find more syzygies. Clearly, its implementation depends on many factors and is out of scope of this extended abstract. Why is it important to know the syzygies?

Algorithm 1 SBA (Signature-based Gröbner Basis Algorithm)

```
Require: Ideal $I = \langle f_1, \ldots, f_m \rangle \subset \mathcal{R}$, monomial order $\leq$ on $\mathcal{R}$, extended to $\mathcal{R}^m$, a rewrite order $\trianglelefteq$ on $\mathcal{G} \cup \mathcal{H}$
Ensure: Signature Gröbner basis $\mathcal{G}$ for $I$, Gröbner basis $\mathcal{H}$ for $\operatorname{syz}(f_1, \ldots, f_m)$
 1: $\mathcal{G} \leftarrow \emptyset, \mathcal{H} \leftarrow \emptyset$
 2: $\mathcal{P} \leftarrow \{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_m\}$
 3: $\mathcal{H} \leftarrow \{f_i \boldsymbol{e}_j - f_j \boldsymbol{e}_i \mid 1 \leq i < j \leq m\} \subset \mathcal{R}^m$
 4: while $\mathcal{P} \neq \emptyset$ do
 5:     $\gamma = a\alpha - b\beta \leftarrow$ element of minimal signature w.r.t. $\leq$ from $\mathcal{P}$
 6:     $\mathcal{P} \leftarrow \mathcal{P} \setminus \{\gamma\}$
 7:     if ($a\alpha$ is not rewritable) and ($b\beta$ is not rewritable) then      // Rewritten criterion (Lemma 8)
 8:         $\gamma \leftarrow$ result of regular $\mathfrak{s}$-reducing $\beta$
 9:         if $\overline{\gamma} = 0$ then
10:             $\mathcal{H} \leftarrow \mathcal{H} + \{\gamma\}$
11:         else
12:             $\mathcal{P} \leftarrow \mathcal{P} \cup \{\operatorname{spair}(\alpha, \gamma) \mid \alpha \in \mathcal{G}, \operatorname{spair}(\alpha, \gamma) \text{ regular}\}$
13:             $\mathcal{G} \leftarrow \mathcal{G} \cup \{\gamma\}$
14:             UpdateSyz $(\mathcal{G}, \mathcal{H})$
15: return $(\mathcal{G}, \mathcal{H})$
```

Lemma 8 (Rewritten criterion)**.** *For signature T* **SBA** *needs to handle exactly one $a\alpha \in \mathcal{R}^m$ from the set $\mathcal{C}_T = \{a\alpha \mid \alpha \in \mathcal{G} \cup \mathcal{H}, a \in \mathcal{M}$ and $\mathfrak{s}(a\alpha) = T\}$.*

Usually the Rewritten criterion as stated above is only defined for $\alpha \in \mathcal{G}$. The so-called **F5** *criterion* or *Syzygy criterion* is also included in Lemma 8: $\alpha \in \mathcal{H}$ means that α is a syzygy and its signature is equal to the lead term in $\mathcal{R}^m$. Clearly, whenever in a situation such that $\alpha \in \mathcal{H}$ and $a\alpha \in \mathcal{C}_T$ we choose $\alpha \in \mathcal{H}$ in $\mathcal{C}_T$, since then we do not need to do any computation in signature $T = \mathfrak{s}(a\alpha)$. The choice in Lemma 8 depends on a rewrite order $\trianglelefteq$:

Definition 9. *A* rewrite order $\trianglelefteq$ *is a total order on* $\mathcal{G}$ *such that* $\mathfrak{s}(\alpha) \mid \mathfrak{s}(\beta) \Rightarrow \alpha \trianglelefteq \beta$.

Thus it is well-defined to choose $\max_{\trianglelefteq} \mathcal{C}_T$ and all other corresponding S-pairs in signature T can be removed. Defining good and efficient rewrite orders is a field of active research.

5. Experimental results

In the following we present the results of the implementation of efficient variants of **SBA** in SINGULAR. All computations were done on an INTEL® XEON® X5460 @ 3.16GHz processor with 64 GB of RAM. **STD** denotes the standard Gröbner basis implementation in SINGULAR based on [12]. $\mathrm{Random}(r, 2, 2)$ denotes dense affine, random systems with r generators in a polynomial ring with r variables, all of degree 2. Similar $\mathrm{HRandom}$ denotes homogeneous systems.

We see in Figure 1 that all variants of **SBA** always compute less zero reductions than **STD**. Besides the affine `cyclic-8` example **SBA** w.r.t $<_{\text{lt-pot}}$ is faster than **STD**, often several times. Currently we are working on further improvements for **SBA**, especially in terms of using **F4**-style linear algebra for the $\mathfrak{s}$-reduction process.

Benchmark	STD	SBA $<_{\text{pot}}$	SBA $<_{\text{d-pot}}$	SBA $<_{\text{lt-pot}}$
cyclic-8	4,284	243	243	671
cyclic-8-h	5,843	243	243	671
eco-11	3,476	0	749	749
eco-11-h	5,429	502	502	749
katsura-11	3,933	0	0	353
katsura-11-h	3,933	0	0	353
noon-9	25,508	0	0	682
noon-9-h	25,508	0	0	682
$\mathrm{Random}(11,2,2)$	6,292	0	0	590
$\mathrm{HRandom}(11,2,2)$	6,292	0	0	590
$\mathrm{Random}(12,2,2)$	13,576	0	0	1,083
$\mathrm{HRandom}(12,2,2)$	13,576	0	0	1,083

(A) Number of zero reductions

Benchmark	STD	SBA $<_{\text{pot}}$	SBA $<_{\text{d-pot}}$	SBA $<_{\text{lt-pot}}$
cyclic-8	32.480	44.310	100.780	38.120
cyclic-8-h	38.300	35.770	98.440	32.640
eco-11	28.450	3.450	27.360	13.270
eco-11-h	20.630	11.600	14.840	7.960
katsura-11	54.780	35.720	31.010	11.790
katsura-11-h	51.260	34.080	32.590	17.230
noon-9	29.730	12.940	14.620	15.220
noon-9-h	34.410	17.850	20.090	20.510
$\mathrm{Random}(11,2,2)$	267.810	77.430	130.400	28.640
$\mathrm{HRandom}(11,2,2)$	22.970	14.060	39.320	3.540
$\mathrm{Random}(12,2,2)$	2,069.890	537.340	1,062.390	176.920
$\mathrm{HRandom}(12,2,2)$	172.910	112.420	331.680	22.060

(B) Time in seconds

FIGURE 1. Experimental results for SINGULAR $4-0-0$

References

[1] Arri, A. and Perry, J. The F5 Criterion revised. *Journal of Symbolic Computation*, 46(2):1017–1029, June 2011. Preprint online at `arxiv.org/abs/1012.3664`.

[2] Buchberger, B. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*. PhD thesis, University of Innsbruck, 1965.

[3] Buchberger, B. A criterion for detecting unnecessary reductions in the construction of Gröbner bases. In *EUROSAM '79, An International Symposium on Symbolic and Algebraic Manipulation*, volume 72 of *Lecture Notes in Computer Science*, pages 3–21. Springer, 1979.

[4] Buchberger, B. Gröbner Bases: An Algorithmic Method in Polynomial Ideal Theory. pages 184–232, 1985.

[5] Decker, W., Greuel, G.-M., Pfister, G., and Schönemann, H. SINGULAR *4-0-0 — A computer algebra system for polynomial computations*, 2014. `http://www.singular.uni-kl.de`.

[6] Eder, C. and Perry, J. F5C: A Variant of Faugère's F5 Algorithm with reduced Gröbner bases. *Journal of Symbolic Computation, MEGA 2009 special issue*, 45(12):1442–1458, 2010. `dx.doi.org/10.1016/j.jsc.2010.06.019`.

[7] Eder, C. and Roune, B. H. Signature Rewriting in Gröbner Basis Computation. In *ISSAC 2013: Proceedings of the 2013 international symposium on Symbolic and algebraic computation*, pages 331–338, 2013.

[8] Faugère, J.-C. A new efficient algorithm for computing Gröbner bases (F4). *Journal of Pure and Applied Algebra*, 139(1–3):61–88, June 1999. `http://www-salsa.lip6.fr/~jcf/Papers/F99a.pdf`.

[9] Faugère, J.-C. A new efficient algorithm for computing Gröbner bases without reduction to zero F5. In *ISSAC'02, Villeneuve d'Ascq, France*, pages 75–82, July 2002. Revised version from `http://fgbrs.lip6.fr/jcf/Publications/index.html`.

[10] Galkin, V. Termination of original F5. `http://arxiv.org/abs/1203.2402`, 2012.

[11] Gao, S., Volny IV, F., and Wang, D. A new algorithm for computing Groebner bases (rev. 2011). `http://www.math.clemson.edu/~sgao/papers/gvw_R130704.pdf`, 2013.

[12] Gebauer, R. and Möller, H. M. On an installation of Buchberger's algorithm. *Journal of Symbolic Computation*, 6(2-3):275–286, October/December 1988.

[13] Roune, B. H. and Stillman, M. Practical Gröbner Basis Computation. In *ISSAC 2012: Proceedings of the 2012 international symposium on Symbolic and algebraic computation*, 2012.

[14] Roune, B. H. and Stillman, M. Practical Gröbner Basis Computation. `http://arxiv.org/abs/1206.6940`, 2012.

University of Kaiserslautern
E-mail address: `ederc @ mathematik.uni-kl.de`

FORMULATING PROBLEMS FOR REAL ALGEBRAIC GEOMETRY

MATTHEW ENGLAND

ABSTRACT. We discuss issues of problem formulation for algorithms in real algebraic geometry, focussing on quantifier elimination by cylindrical algebraic decomposition. We recall how the variable ordering used can have a profound effect on both performance and output and summarise what may be done to assist with this choice. We then survey other questions of problem formulation and algorithm optimisation that have become pertinent following advances in CAD theory, including both work that is already published and work that is currently underway. With implementations now in reach of real world applications and new theory meaning algorithms are far more sensitive to the input, our thesis is that intelligently formulating problems for algorithms, and indeed choosing the correct algorithm variant for a problem, is key to improving the practical use of both quantifier elimination and symbolic real algebraic geometry in general.

1. INTRODUCTION

We will discuss the effect problem formulation can have on the use of symbolic algorithms for real algebraic geometry. This follows our recent work on cylindrical algebraic decomposition, one of the most important algorithms in this field. We discuss the issue of variable ordering, well known to play a key role, but also survey a number of other issues that are now pertinent.

Let $Q_i \in \{\exists, \forall\}$ and ϕ be some quantifier-free formula. Then given

$$\Phi := Q_{k+1}x_{k+1} \ldots Q_n x_n \, \phi(x_1, \ldots, x_n),$$

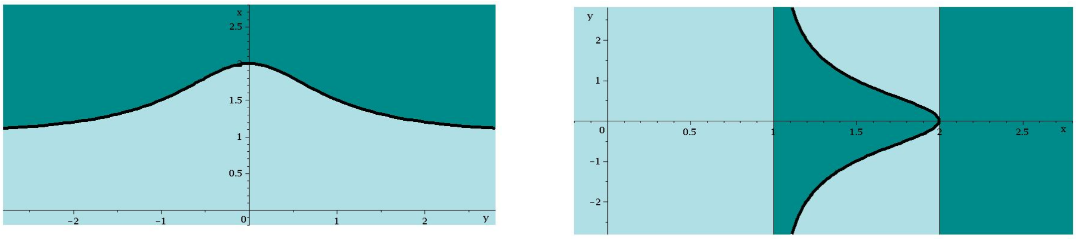
quantifier elimination (QE) is the problem of producing $\psi(x_1, \ldots, x_k)$, a quantifier-free formulae equivalent to Φ. In the case $k = 0$ we have a *decision problem*: is Φ true? Tarski proved that QE is always possible for semi-algebraic formulae (polynomials and inequalities) over $\mathbb{R}$ [13]. The complexity of Tarski's method is indescribable as a finite tower of exponentials and so when Collins gave an alternative with cylindrical algebraic decomposition (CAD) [7] it was a major breakthrough despite complexity doubly exponential in the number of variables. CAD implementations remain the best option for many classes of problems.

Collins' CAD algorithm works in two stages. First *projection* calculates sets of projection polynomials S_i in variables $(x_1, \ldots, x_i)$ by applying an operator recursively starting with the polynomials from ϕ. Then in the *lifting* stage decompositions of real space in increasing dimensions are formed from the roots of those polynomials. First, the real line is decomposed according to the roots of the univariate polynomials. Then over each cell c in that decomposition the bivariate polynomials are taken at a sample point and a decomposition of $c \times \mathbb{R}$ is produced according to their roots. Taking the union gives the decomposition of $\mathbb{R}^2$ and we proceed this way to a decomposition of $\mathbb{R}^n$. The decompositions are cylindrical (projections of any two cells onto the first k coordinates are either identical or disjoint) and each cell is a semi-algebraic set (described by polynomial relations).

Collins' original algorithm uses a projection operator which guarantees CADs of $\mathbb{R}^n$ on which the polynomials in ϕ have constant sign, and thus Φ constant truth value, on each cell. Hence only a sample point from each cell needs to be tested and the equivalent quantifier free formula ψ can be generated from the semi-algebraic sets defining the cells in the CAD of $\mathbb{R}^k$ for which Φ is true. There have been numerous improvements, optimisations and extensions of CAD since Collins' work (with a summary of the first 20 years given in [8]).

2. Variable ordering

When using CAD for QE we must project quantified variables first, but we are free to project the other variables in any order (and to change the order within quantifier blocks). The variable ordering used can make a big difference. For example, let $f := (x-1)(y^2+1)-1$ and consider the two minimal CADs visualised below. In each case we project down with the left figure projecting x first and the right y. In this case we see that wrong choice more than doubles the number of cells. Of course, this is just a toy example, but [5] defined a class of examples where changing variable ordering would change the number of cells required from constant to doubly exponential in the number of variables.



Various heuristics exist to help choose a good variable ordering:

Brown: Eliminate lowest degree variable first (with tie-breaking rules) [4, Section 5.2]. Quite effective but considers only the initial input rather than the full projection set.

sotd: For all admissible orderings, calculate the projection set and choose the one with smallest *sum of total degree* [9]. Performs well but costly with many orderings.

Greedy sotd: Allocate one variable of the ordering at a time by projecting each unallocated variable and choosing the one which increases the sotd least [9].

ndrr: The sotd based heuristics can be misled, or give ties, especially when the differences lie in the real geometry. In this case we can compare the *number of distinct real roots* of the univariate projection polynomials [3] (the first step of lifting).

Machine Learning: Essentially a meta-heuristic on the above [11].

3. Other questions of input formulation

A key improvement to CAD is the development of projection operators that guarantee only truth invariance of ϕ, rather than sign-invariance of the polynomials within. This is achieved by considering the logical structure of ϕ, but brings in sensitivity to such structure.

Designating ECs: An *equational constraint* (EC) is an equation logically implied by a formula. The algorithm in [12] builds a CAD relative to a designated EC which is sign-invariant for the polynomial defining the EC, and for the other polynomials only when the EC is satisfied. If a formula has more than one EC, which to designate?

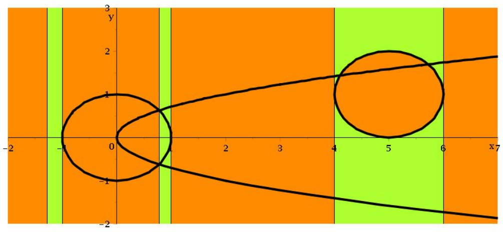
Sub-formulae for TTICAD: In [2] a truth-table invariant CAD (TTICAD) was defined as a CAD on whose cells the truth-table for a set of formulae is invariant. A new operator was presented which takes advantage of ECs in the separate formulae. If any formula has more than one EC then we have the issue above again. Further, TTICAD can be used to find a truth-invariant CAD for a single formula by breaking it up into sub-formulae, but how best to do this?

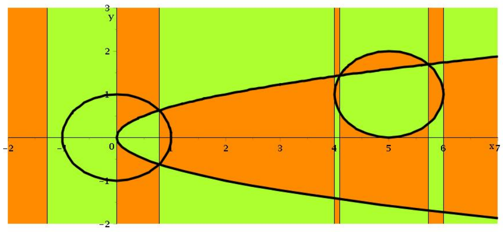
Experimental results in [2] suggested the heuristics above can also help with these questions, but when the issues are combined the number of possibilities can become overwhelming. Further, there are additional issues where the existing heuristics are of no help.

Order to process constraints: In [1] a new TTICAD algorithm is presented which is sensitive to the order in which constraints are considered. The images below represent two TTICADs relative to a formula defined by the polynomials graphed. The difference is caused solely by this ordering with the one on the right having three times more cells. In [10] new heuristics are developed to help with this choice.

Implicit ECs: Consider $\phi := (f_1 = 0 \wedge \phi_1) \vee (f_2 = 0 \wedge \phi_2)$. There is no explicit EC but the formula is logically equal to $(f_1 f_2 = 0) \wedge \phi$. Using this gives the benefit of the reduced projection set and thus less cells, but the increase in polynomial degrees may have an impact on timings.

Well-orientedness: Some CAD algorithms only work on input that is *well-oriented*. The precise details of this condition varies between algorithms and it is possible for input to be well-oriented for one but not another. This raises the question of whether a good choice can be made at the start, or if partial calculations can be reused?





4. Formulating problems, preprocessing and algorithm choice

Finally, we remark on some related issues which have come to light recently.

Precondition input: In [15] the idea of preconditioning the input to CAD using Groebner bases was investigated, with [2] extending this to TTICAD. The former found that this could be extremely beneficial, but not universally so. A heuristic was developed to identify when, but [2] found this was not suitable for TTICAD.

Deriving the mathematics: In [14] a long standing motion planning problem was solved using CAD by changing the analysis used to formulate the input formula. Instead of a description of the feasible region a negation of one for the infeasible region was used. Such a reformulation was easy to do but made a great difference to the feasibility of CAD. How can we identify such benefits in general?

Algorithm choice: Recently an alternative to the projection and lifting approach to CAD has been investigated, in which a decomposition of complex space is first built using triangular decompositions and regular chains theory [6] (this was how the TTICAD algorithm in [1] differed from [2]). Experiments in [6] and [1] show that the different approaches outperform each other for different examples. How can we classify examples for use with one approach or the other?

5. Conclusions

We have summarised issues of problem formulation which can dramatically affect the performance of CAD. In some cases heuristics have been developed to help, but there is still much work to be done in making these practical and in extending them to the currently unanswered questions. It is likely that much of what is learned here could be used throughout QE, or more generally for symbolic algebraic geometry.

References

[1] R. Bradford, C. Chen, J.H. Davenport, M. England, M. Moreno Maza, and D. Wilson. Truth table invariant cylindrical algebraic decomposition by regular chains. Preprint: `arxiv:1401.6310`

[2] R. Bradford, J.H. Davenport, M. England, S. McCallum, and D. Wilson. Cylindrical algebraic decompositions for boolean combinations. In *Proc. ISSAC '13*, pages 125–132. ACM, 2013.

[3] R. Bradford, J.H. Davenport, M. England, and D. Wilson. Optimising problem formulations for cylindrical algebraic decomposition. In *Intelligent Computer Mathematics* (LNCS 7961), pages 19–34. Springer Berlin Heidelberg, 2013.

[4] C.W. Brown. Companion to the tutorial: Cylindrical algebraic decomposition, presented at ISSAC '04. `http://www.usna.edu/Users/cs/wcbrown/research/ISSAC04/handout.pdf`, 2004.

[5] C.W. Brown and J.H. Davenport. The complexity of quantifier elimination and cylindrical algebraic decomposition. In *Proc. ISSAC '07*, pages 54–60. ACM, 2007.

[6] C. Chen and M. Moreno Maza. An incremental algorithm for computing cylindrical algebraic decompositions. *Proc. ASCM '12*. To appear in LNAI, Springer. Preprint: `arxiv:1210.5543`, 2012.

[7] G.E. Collins. Quantifier elimination for real closed fields by cylindrical algebraic decomposition. In *Proc. 2nd GI Conference on Automata Theory and Formal Languages*, pages 134–183. Springer-Verlag, 1975.

[8] G.E. Collins. Quantifier elimination by cylindrical algebraic decomposition – 20 years of progress. In *Quantifier Elimination and Cylindrical Algebraic Decomposition*, pages 8–23. Springer-Verlag, 1998.

[9] A. Dolzmann, A. Seidl, and T. Sturm. Efficient projection orders for CAD. In *Proc. ISSAC '04*, pages 111–118. ACM, 2004.

[10] M. England, R. Bradford, C. Chen, J.H. Davenport, M. Moreno Maza, and D. Wilson. Problem formulation for truth-table invariant cylindrical algebraic decomposition by incremental triangular decomposition. To appear *Proc. CICM '14*, 2014. Preprint: `arxiv:1404.6371`

[11] Z. Huang, M. England, D. Wilson, J.H. Davenport, L. Paulson, and J. Bridge. Applying machine learning to the problem of choosing a heuristic to select the variable ordering for cylindrical algebraic decomposition. To appear *Proc. CICM '14*, 2014. Preprint: `arxiv:1404.6369`

[12] S. McCallum. On projection in CAD-based quantifier elimination with equational constraint. In *Proc. ISSAC '99*, pages 145–149. ACM, 1999.

[13] A. Tarski. A decision method for elementary algebra and geometry. In *Quantifier Elimination and Cylindrical Algebraic Decomposition*, pages 24–84. Springer-Verlag, 1998.

[14] D. Wilson, J.H. Davenport, M. England, and R. Bradford. A "piano movers" problem reformulated. In *Proc. SYNASC '13*. IEEE, 2013.

[15] D.J. Wilson, R.J. Bradford, and J.H. Davenport. Speeding up cylindrical algebraic decomposition by Gröbner bases. In *Intelligent Computer Mathematics* (LNCS 7362), pages 280–294. Springer, 2012.

University of Bath, UK.
E-mail address: `M.England@bath.ac.uk`

DETERMINANT OF ANY MATRIX THAT BELONGS TO Z(J)

JOSEP FERRER, DAVID MINGUEZA, AND M.EULÀLIA MONTORO

ABSTRACT. Given a Jordan matrix J, we obtain an explicit formula for the determinant of any matrix T that commutes with it and some applications are given. This work is partially published in [2].

INTRODUCTION

Let $\mathbb{F}$ be an arbitrary field, $M_n(\mathbb{F})$ the set of all matrices $n \times n$ over $\mathbb{F}$ and $J \in M_n(\mathbb{F})$ a Jordan matrix. We obtain an explicit formula for the determinant of any matrix that commutes with J, i.e., the determinant of any element $T \in Z(J)$, the centralizer of J. Our result can also be extended to any $T' \in Z(A)$, where $A \in M_n(\mathbb{F})$ can be reduced to $J = S^{-1}AS$. This is because $T = S^{-1}T'S \in Z(J)$, and clearly $\det T' = \det T$. If $\mathbb{F}$ is algebraically closed, any matrix A can be reduced in this way to a suitable J. In order to achieve our main result, we use an alternative canonical form $W \in M_n(\mathbb{F})$ called the Weyr canonical form. This canonical form has the advantage that all matrices $K \in Z(W)$ are upper block triangular. The permutation similarity of $T \in Z(J)$ and $K \in Z(W)$ is exploited to obtain a formula for the determinant of T.

1. PRELIMINARIES

We will assume throughout all paper that J has only one eigenvalue λ and write $\alpha = (\alpha_1, \dots, \alpha_m)$ for the Segre characteristic of J. That is to say, $m = \dim\ker(J - \lambda I_n)$, and $\alpha_1 \geq \cdots \geq \alpha_m$ are the sizes of the Jordan blocks. For convenience, we will consider the matrices $T \in Z(J)$ block-partitioned according to the following indices:

Definition 1.1. If $n_1 > \ldots > n_\tau$ are the different sizes in the partition α and $s_1, \dots, s_\tau$ are defined as how many times each size $n_1, \dots, n_\tau$ is repeated in α, then we define the tuples associated to α as:

$$\begin{aligned} N(\alpha) &= (n_1, \dots, n_\tau), \\ S(\alpha) &= (s_1, \dots, s_\tau), \\ D(\alpha) &= (d_1, d_2, \dots, d_{\tau-1}, d_\tau), \end{aligned} \tag{1}$$

with $d_i = n_i - n_{i+1}$, $1 \leq i \leq \tau - 1$ and $d_\tau = n_\tau$.

Example 1.2. If $\alpha = (5, 2, 2, 1)$ then, $\tau = 3$, $N(\alpha) = (5, 2, 1)$, $S(\alpha) = (1, 2, 1)$, $D(\alpha) = (3, 1, 1)$.

A key tool to compute $\det T$ is an alternative canonical form of J called the Weyr form (see [4]). In order to do this, we consider the conjugate partition $\omega = (\omega_1, \dots, \omega_{\alpha_1})$ of $\alpha = (\alpha_1, \dots, \alpha_m)$.

Remark 1.3. By the standard properties of Young's diagrams, it is clear that:

$$\begin{aligned} N(\omega) &= (S_\tau, S_{\tau-1}, \dots, S_1) \\ S(\omega) &= (d_\tau, d_{\tau-1}, \dots, d_1) \\ D(\omega) &= (s_\tau, \dots, s_1) \end{aligned} \tag{2}$$

where $S_i = \sum_{j=1}^{i} s_j$.

2. The centralizer of a Jordan Matrix

It is well known that matrices $T \in Z(J)$ can be described in terms of square or rectangular Toeplitz matrices.

Definition 2.1. If $T_i \in M_i(\mathbb{F})$ is a Lower triangular Toeplitz matrix, then:

1) For $i > j$, we denote by $TD_{i,j} \in M_{i\times j}(\mathbb{F})$ (Down Toeplitz matrix) the following matrix:

$$TD_{i,j} := \begin{bmatrix} \mathbb{O} \\ T_j \end{bmatrix}$$

2) For $i < j$, we denote by $TL_{i,j} \in M_{i\times j}(\mathbb{F})$ (Left Toeplitz matrix) the following matrix:

$$TL_{i,j} := \begin{bmatrix} T_i & \mathbb{O} \end{bmatrix}$$

Using the notation in Definition 1.1, we can regroup the block-partitions by joining the diagonal blocks of the same size and the following characterization for matrices $T \in Z(J)$ is considered.

Theorem 2.2. ([3]) Every matrix $T \in Z(J)$ can be written as:

$$T = \begin{bmatrix} T_{1,1} & \dots & T_{1,\tau} \\ \vdots & \ddots & \vdots \\ T_{\tau,1} & \dots & T_{\tau,\tau} \end{bmatrix} \tag{3}$$

where $T_{i,j} \in M_{n_i s_i \times n_j s_j}(\mathbb{F})$ for $1 \le i, j \le \tau$ are:

1) If $i = j$, then $T_{i,i}$ is block-partitioned into $s_i \times s_i$ Lower Triangular Toeplitz matrices.
2) If $i < j$, then $T_{i,j}$ is block-partitioned into $s_i \times s_j$ Down Toeplitz matrices.
3) If $i > j$, then $T_{i,j}$ is block-partitioned into $s_i \times s_j$ Left Toeplitz matrices.

3. The centralizer of a Weyr matrix

Rearranging the Jordan basis according to $\omega = (\omega_1, \dots, \omega_{\alpha_1})$, the conjugate partition of $\alpha = (\alpha_1, \dots, \alpha_m)$, the Weyr canonical form is obtained. We recall its definition (see, for instance, [4]):

Definition 3.1. The Weyr matrix with eigenvalue λ associated to the partition $\omega = (\omega_1, \dots, \omega_{\alpha_1})$ is the $n \times n$ matrix W, block-partitioned as $\alpha_1 \times \alpha_1$ matrices $W_{i,j} \in M_{\omega_i \times \omega_j}(\mathbb{F})$ in the following form:

(1) The main diagonal blocks $W_{i,i}$ are the $\omega_i \times \omega_i$ scalar matrices λI_{ω_i} for $i = 1, \dots, \alpha_1$.
(2) The first superdiagonal blocks $W_{i,i+1}$ are full column-rank $\omega_i \times \omega_{i+1}$ matrices in reduced row-echelon form (that is, an identity matrix followed by zero rows) for $i = 1 \dots, n_1 - 1$.
(3) All other blocks are zero.

In the following proposition we recall the description of matrices that commute with a given Weyr matrix W (see [4]), in particular we focus in the diagonal blocks of such matrices.

Proposition 3.2. *If $W \in M_n(\mathbb{F})$ is a Weyr matrix with eigenvalue λ associated to the partition $\omega = (\omega_1, \ldots, \omega_{\alpha_1})$ then, using the notation of Definition 1.1 and Remark 1.3, all matrices $K \in Z(W)$ are of the form:*

$$K = \begin{bmatrix} \tilde{K}_{1,1} & \tilde{K}_{1,2} & \ldots & \tilde{K}_{1,\tau} \\ 0 & \tilde{K}_{2,2} & \ldots & \tilde{K}_{2,\tau} \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \ldots & 0 & \tilde{K}_{\tau,\tau} \end{bmatrix} \tag{4}$$

where each $\tilde{K}_{j,j}$ is a block-partitioned matrix, with the same matrix $K'_j \in M_{S_{\tau-j+1}}(\mathbb{F})$ repeated $d_{\tau-j+1}$ times in the diagonal, i.e.

$$\tilde{K}_{j,j} = \begin{bmatrix} K'_j & \ldots & \ldots & \ldots \\ 0 & K'_j & \ldots & \ldots \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \ldots & 0 & K'_j \end{bmatrix}. \tag{5}$$

And each K'_j can be expressed as:

$$K'_j = \begin{bmatrix} K''_{s_1} & \ldots & \ldots & \ldots \\ 0 & K''_{s_2} & \ldots & \ldots \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \ldots & 0 & K''_{s_{\tau-j+1}} \end{bmatrix} \in M_{S_{\tau-j+1}}(\mathbb{F}), \tag{6}$$

where $K''_{s_j} \in M_{s_j}(\mathbb{F})$.

4. Computing the determinant of any $T \in Z(J)$

Let $J \in M_n(\mathbb{F})$ be a Jordan matrix with an unique eigenvalue and W the Weyr matrix of J. We write as above $\alpha = (\alpha_1, \ldots, \alpha_m)$ and $\omega = (\omega_1, \ldots, \omega_{\alpha_1})$, the Segre and the Weyr characteristic of J respectively. Moreover, $N(\alpha) = (n_1, \ldots, n_\tau)$ and $S(\alpha) = (s_1, \ldots, s_\tau)$ are as in Definition 1.1.

First, we consider a particular case. Given $T_{k,k}$ as in Theorem 2.2, that is:

$$T_{k,k} = \begin{bmatrix} T^{1,1}_{n_k} & \ldots & T^{1,s_k}_{n_k} \\ \vdots & \ddots & \vdots \\ T^{s_k,1}_{n_k} & \ldots & T^{s_k,s_k}_{n_k} \end{bmatrix} \text{ where } T^{i,j}_{n_k} = \begin{bmatrix} x^{i,j}_1 & 0 \ldots & 0 \\ \vdots & \ddots & \vdots \\ x^{i,j}_{n_k} & \ldots & x^{i,j}_1 \end{bmatrix}, 1 \leq i,j \leq s_k.$$

Lemma 4.1. *Using the above notation:*

$$\det(T_{k,k}) = \left(\det \begin{bmatrix} x^{1,1}_1 & \ldots & x^{1,s_k}_1 \\ \vdots & \ddots & \vdots \\ x^{s_k,1}_1 & \ldots & x^{s_k,s_k}_1 \end{bmatrix} \right)^{n_k} \tag{7}$$

In particular, this determinant depends only on s_k^2 variables.

Since any $K \in Z(W)$ is a block-partitioned upper triangular matrix, we can obtain as a corollary of Proposition 3.2 the determinant of K which will be a key point in the proof of Theorem 4.3.

Corollary 4.2. *Using the notations of Proposition 3.2, given any $K \in Z(W)$ we have that:*

$$\det K = (\det K''_{s_1})^{n_1} \cdots (\det K''_{s_\tau})^{n_\tau} \tag{8}$$

In particular, this determinant depends only on $s = s_1^2 + \ldots + s_\tau^2$ variables.

Given any $T \in Z(J)$, the following theorem gives a formula for $\det(T)$.

Theorem 4.3. *Let $T \in Z(J)$ be block-partitioned as in Theorem 2.2, then*

$$\det T = \det T_{1,1} \cdots \det T_{\tau,\tau},$$

and each of the $\det T_{i,i}$, $1 \leq i \leq \tau$, can been computed as in Lemma 4.1.

Corollary 4.4. *The determinant of a matrix $T \in Z(J)$ only depends on the elements in the diagonal of the square blocks of T.*

Example 4.5. If J is a Jordan matrix with an unique eigenvalue λ and Segre characteristic $\alpha = (3, 3, 2, 2, 2, 1)$. Then, $\dim Z(J) = 65$ but if $T(x_1, \ldots, x_{65})$ is the parametrized form of $Z(J)$, $\det T(x_1, \ldots, x_{65})$ only depends on 14 variables.

5. Application

Given a matrix $A \in M_n(\mathbb{F})$, an $A-$invariant subspace $V \subset \mathbb{F}^n$ is an *hyperinvariant subspace* if is also invariant for all matrices that commute with A and is a *characteristic subspace* if is invariant for all non-singular matrices that commute with A. It is known (see [1]) that if $\mathbb{F} \neq GF(2)$ the lattices of hyperinvariant subspaces and characteristic subspaces of A coincides. If $\mathbb{F} = GF(2)$, then there exist characteristic non hyperinvariant subspaces. In the characterization of such subspaces is important to know when a matrix $T \in Z(J)$ is non-singular. In particular, as a corollary of Theorem 4.3:

Corollary 5.1. *Let $J \in M_n(GF(2))$ be a nilpotent Jordan matrix with Segre characteristic $\alpha = (\alpha_1, \ldots, \alpha_m)$. Let us denote by $\Omega = \{i = 1, \ldots, \tau | s_i = 1\}$, where s_i is as in Definition 1.1, then:*

$$T \in Z(J) \textit{ non-singular} \Rightarrow \det T = \prod_{i \notin \Omega} \det T_{i,i} \tag{9}$$

References

[1] P. Astuti, H.K. Wimmer. *Hyperinvariant, characteristic and marked subspaces.* Oper. Matrices,3, pp. 261-270, (2009).

[2] J.Ferrer, D. Mingueza, M.E. Montoro. *Determinant of a matrix that commutes with a Jordan matrix.* Linear Algebra and its Applications, 439 (12), pp. 3945 - 3954, (2013).

[3] I. Gohberg, P. Lancaster, L. Rodman. *Invariant subspaces of matrices with applications.* SIAM, 1986.

[4] K.C. O'Meara, J. Clark, C. I. Vinsonhaler. *Advanced Topics In Linear Algebra : Weaving Matrix Problems Through the Weyr Form.* Oxford: Oxford University Press, 2011.

Universitat Politècnica de Catalunya
E-mail address: josep.ferrer@upc.edu

Accenture
E-mail address: david.mingueza@ya.com

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

BOND THEORY FOR PENTAPODS AND HEXAPODS

MATTEO GALLET, GEORG NAWRATIL, AND JOSEF SCHICHO

ABSTRACT. This paper deals with the old and classical problem of determining necessary conditions for the overconstrained mobility of some mechanical device. Methods from algebraic geometry have already been used to investigate these mobility conditions, and we propose some tools specifically developed for the so–called n–pods. In particular, we focus on the conditions which are imposed on an n–pod by the existence of points of particular kind, which lie on the boundary of the set of self–motions of the n–pod when we consider a specific compactification of the group of direct isometries of $\mathbb{R}^3$. Furthermore we set up a photogrammetry–like technique which allows to establish necessary conditions for movability of 5–pods.

INTRODUCTION

The objects we focus on in this paper are mechanical manipulators called *n–pods*. As described in [2], the geometry of this kind of devices is defined by the coordinates of the n base anchor points $p_i = (a_i, b_i, c_i) \in \mathbb{R}^3$ and of the n platform anchor points $P_i = (A_i, B_i, C_i) \in \mathbb{R}^3$ in one of their possible configurations. All pairs of points (p_i, P_i) are connected by a rigid body, called *leg*, so that for all possible configurations the distance $d_i = \|p_i - P_i\|$ is preserved.

Notation. We think of an n–pod L as a triple

$$L = \Big((p_1, \ldots, p_n), (P_1, \ldots, P_n), (d_1, \ldots, d_n) \Big)$$

where p_i, P_i and d_i are defined as above.

We are interested in describing the *self–motions* of a given n–pod L, namely which direct isometries σ of $\mathbb{R}^3$ satisfy the condition

$$\|\sigma(p_i) - P_i\| \;=\; \|p_i - P_i\| \;=\; d_i \qquad \text{for all } i \in \{1, \ldots, n\} \tag{1}$$

In particular we want to understand what is the *dimension* of the set of these isometries, namely the *mobility* of L, and what conditions we have to impose on the base and platform points to reach a prescribed mobility.

We first study some geometric properties of the group of direct isometries of $\mathbb{R}^3$, and in particular we notice that it is possible to embed it in projective space in a way specifically tuned for dealing with n–pods (Section 1). At this point, we prove that the inspection of boundary points of the set of self–motions of an n–pod L gives information on base and platform points (Section 2). Eventually, we develop a photogrammetry theory based on identifications (under Möbius transformations) of 2D projections of 3D configurations of points, and we use it to establish a result on pentapods with mobility 2 (Section 3).

Kinematical main results. From the kinematical point of view this paper contains the following two main results:

Result 1. *If the mobility of a pentapod is* 2 *or higher, then one of the following conditions holds:*

(a) *The platform and the base are similar.*
(b) *The platform and the base are planar and affine equivalent.*
(c) *There exists* $m \leq 5$ *such that* $p_1, \ldots, p_m$ *are collinear and* $P_{m+1}, \ldots, P_5$ *are equal, up to permutation of indices and interchange of platform and base.*

Result 2. *If an* n*–pod is mobile, then one of the following conditions holds:*

(i) *There exists at least one pair of orthogonal projections* π_l *and* π_r *such that the projections of the platform points* $p_1, \ldots, p_n$ *by* π_l *and of the base points* $P_1, \ldots, P_n$ *by* π_r *are Möbius equivalent.*
(ii) *There exists* $m \leq n$ *such that* $p_1, \ldots, p_m$ *are collinear and* $P_{m+1}, \ldots, P_n$ *are collinear, up to permutation of indices.*

1. A NEW COMPACTIFICATION OF SE_3

The elements of the group SE_3 of direct isometries of $\mathbb{R}^3$ correspond bijectively to points in an open subset of the Study quadric in $\mathbb{P}^7_{\mathbb{R}}$ (where we take as coordinates the so–called Study parameters of the isometries), defined as the set $\big\{e_0 f_0 + e_1 f_1 + e_2 f_2 + e_3 f_3 = 0\big\}$. This embedding of SE_3 turns out to be very useful in the study of mobility properties of objects coming from kinematics. However, in our situation a different compactification will lead us to a better comprehension of the phenomena which can appear. We introduce another projective embedding of (the complexification of) SE_3 considering the following polynomials:

$$\begin{cases} n_0 = f_0^2 + f_1^2 + f_2^2 + f_3^2, & \\ c_{ij} = e_i e_j & \text{for } 0 \leq i \leq j \leq 3, \\ b_{ij} = e_i f_j - e_j f_i & \text{for } 0 \leq i < j \leq 3. \end{cases} \tag{2}$$

They give rise to a rational map

$$\Phi : \underbrace{\mathbb{P}^7_{\mathbb{C}}}_{\text{coordinates } (e_0:\ldots:e_3:f_0:\ldots:f_3)} \dashrightarrow \underbrace{\mathbb{P}^{16}_{\mathbb{C}}}_{\text{coordinates } (n_0:\{b_{ij}\}:\{c_{ij}\})}$$

Definition 1.1. We define X to be the Zariski closure of the image of SE_3 (embedded in $\mathbb{P}^7_{\mathbb{C}}$) via Φ.

Lemma 1.2. *The variety* X *is a compactification of* SE_3 *and Equation (1) becomes linear in the new coordinates. We denote by* B *the* boundary *of* X*, namely the set* $X \setminus \mathrm{SE}_3$.

Using the newly created compactification we can define the concepts of *configuration set*, *mobility* (also known as *internal mobility* or *internal degrees of freedom*) and *bond* of an n–pod.

Definition 1.3. The *configuration set* K_L of an n–pod L is defined as:

$$K_L = \big\{\sigma \in \mathrm{SE}_3 \text{ satisfying Equation (1) for all } (p_i, P_i)\big\} \subseteq X$$

The *mobility* of an n–pod L is defined as the dimension of K_L.

Definition 1.4. The set of *bonds* B_L of an n–pod L is defined as the intersection of the Zariski closure of K_L with the boundary B of X.

Remark 1.5. Belonging to the boundary, bonds do not represent direct isometries of $\mathbb{R}^3$, but we will see in Section 2 that we can give a precise geometric meaning to their presence.

The following result is the key tool to prove all theorems in Section 2:

Proposition 1.6. *The natural left and right actions of* SE_3 *on itself extend to linear actions on* X.

2. Geometric interpretation of Bonds

According to the local behavior of the variety X, bonds can be classified into four groups:

inversion bonds: at least one c_{ij}–coordinate is not zero, and $n_0 \neq 0$ (X is smooth at these points);

butterfly bonds: at least one c_{ij}–coordinate is not zero, and $n_0 = 0$ (these are double points of X);

similarity bonds: all c_{ij}–coordinates are zero and the following matrix has rank 2

$$M = \begin{pmatrix} b_{01} & b_{02} & b_{03} & b_{12} & b_{13} & b_{23} \\ b_{23} & -b_{13} & b_{12} & b_{03} & -b_{02} & b_{01} \end{pmatrix}$$

collinearity bonds: all c_{ij}–coordinates are zero and the matrix M has rank 1.

The presence of some kind of bond implies precise conditions on base and platform points of an n–pod. In the following, if $\varepsilon \in S^2$ is a unit vector in $\mathbb{R}^3$, we denote by π_ε the orthogonal parallel projection along ε.

Theorem 2.1. *Assume that $\beta \in B_L$ is an inversion/similarity bond of L. Then there exist directions $l, r \in S^2$ (depending on β) such that, if for $i = 1, \ldots, n$ we set $q_i = \pi_l(p_i)$ and $Q_i = \pi_r(P_i)$, then there is an inversion/similarity of $\mathbb{R}^2$ mapping $q_1, \ldots, q_n$ to $Q_1, \ldots, Q_n$.*

Theorem 2.2. *Assume that $\beta \in B_L$ is a butterfly bond of L. Then there exist directions $l, r \in S^2$ (depending on β) such that, up to permutation of indices $1, \ldots, n$, there exists $m \leq n$ so that $p_1, \ldots, p_m$ are collinear on a line parallel to l, and $P_{m+1}, \ldots, P_n$ are collinear on a line parallel to r.*

Theorem 2.3. *Assume that $\beta \in B_L$ is a collinearity bond of L. Then $p_1, \ldots, p_n$ are collinear or $P_1, \ldots, P_n$ are collinear (or both).*

The technique we adopt to show the previous results is to use left and right actions of SE_3 on X in order to find "good" representatives for the orbits of all kind of bonds, and then to perform explicit computations. Altogether, these theorems give Result 2 presented in the Introduction.

3. Möbius Photogrammetry

This Section deals with a mathematically freestanding problem, which we call *Möbius Photogrammetry*. Unlike traditional photogrammetry, which tries to recover a set of points from a finite collection of central projections, here we consider the problem of reconstructing a vector of 5 points in $\mathbb{R}^3$ starting from finitely many orthogonal parallel projections, assuming that we know them only up to Möbius transformations.

If we denote by M_5 the moduli space of 5 points in $\mathbb{P}^1_{\mathbb{C}}$, and we fix a vector $\vec{A} = (A_1, \ldots, A_5)$ of points in $\mathbb{R}^2$, it is possible to define a *photographic map*

$$f_{\vec{A}} : S^2 \longrightarrow M_5$$

associating to each unit vector $\varepsilon \in S^2$ the equivalence class of the projection along ε of the points in $\vec{A}$. Here we identify the plane $\mathbb{R}^2$, on which the points are projected, with the complex plane $\mathbb{C}$, and we embed the latter in $\mathbb{P}^1_{\mathbb{C}}$. Using the results in [1] we can write down explicitely an embedding $M_5 \subseteq \mathbb{P}^5_{\mathbb{C}}$ and the polynomials defining $f_{\vec{A}}$, and prove the following two lemmata:

Lemma 3.1. *Let $\vec{A} = (A_1, \dots, A_5)$ be a 5–tuple of points that are not coplanar. Then the photographic map $f_{\vec{A}} : S^2 \longrightarrow M_5$ is birational to a rational curve of degree 10 or 8 in M_5.*

Lemma 3.2. *Let $\vec{A} = (A_1, \dots, A_5)$ be a 5–tuple of planar points, not collinear. Then the photographic map $f_{\vec{A}} : S^2 \longrightarrow M_5$ is $2:1$ to a rational curve of degree 5, 4, 3, or 2 in M_5.*

Finally, taking into account the geometrical properties of M_5 (which is a Del Pezzo surface of degree 5) one can prove that the set of images under the photographic map can be used to determine, up to similarities, the vector of points we started with.

Theorem 3.3. *Let $\vec{A}$ and $\vec{B}$ be two 5–tuples of points in $\mathbb{R}^3$ such that no 4 points are collinear. Assume that $f_{\vec{A}}(S^2)$ and $f_{\vec{B}}(S^2)$ are equal as curves in M_5. If $\vec{A}$ is coplanar, then $\vec{B}$ is also coplanar and affine equivalent to $\vec{A}$. If $\vec{A}$ is not coplanar, then $\vec{B}$ is similar to $\vec{A}$.*

Now Theorem 3.3, together with the theorems of Section 2, yields Result 1 of the Introduction (for example, the hypotheses of parts (a) and (b) in Result 1 imply the existence of infinitely many inversion/similarity bonds, which in turn forces the images $f_{\vec{p}}(S^2)$ and $f_{\vec{P}}(S^2)$ to be equal).

REFERENCES

[1] Benjamin Howard, John Millson, Andrew Snowden, and Ravi Vakil. The equations for the moduli space of n points on the line. *Duke Math. J.*, 146(2):175–226, 2009.

[2] Georg Nawratil. Introducing the theory of bonds for Stewart Gough platforms with self-motions. *ASME Journal of Mechanisms and Robotics*, 6(1):011004, 2014.

Matteo Gallet, Research Institute for Symbolic Computation, Johannes Kepler University, Altenberger Straße 69, 4040 Linz, Austria.

E-mail address: mgallet@risc.jku.at

Georg Nawratil, Institute of Discrete Mathematics, and Geometry, Vienna University of Technology, Wiedner Hauptstrasse 8-10/104, 1040 Vienna, Austria.

E-mail address: nawratil@geometrie.tuwien.ac.at

Josef Schicho, Research Institute for Symbolic Computation, Johannes Kepler University, Altenberger Straße 69, 4040 Linz, Austria.

E-mail address: josef.schicho@risc.jku.at

ON DETECTION OF SOLITARY WAVES, USING PHASE DIAGRAMS AND REAL DISCRIMINANT

ANDRÉ GALLIGO, DENYS DUTYKH, AND DIDIER CLAMOND

ABSTRACT. We present an application of Computer algebra to Fluid Mechanics: We investigate “capillary-gravity shallow” solitary waves in the framework of the Serre-Green-Naghdi equations. Our main tool is a real discriminant, used to classify the topological behaviors of a family of plane real curves.

INTRODUCTION

We investigate “capillary-gravity shallow” solitary waves in the framework of the Serre-Green-Naghdi equations. See [Serre, DCMM]. The governing equations take into account an effect of capillarity pressure quantified by a Bond number Bo (depending on a tension surface coefficient) and an effect of gravity force, jointly quantified by a Fround number Fr, which also indicates the wave phase velocity.

To simplify the notations, we let $a = Fr^2$ and $b = Bo$. For physical reasons, we can concentrate on the cases where $a \in [0, 2]$ and $b \in [0, 2]$. The variable x indicates the abscissa in the channel, the principal unknowns are the elevation $h(x)$ of the free surface above x, and $\bar{u}(x)$ the depth-averaged horizontal velocity. The height of the surface at rest is normalized to 1; $h = 1$ is therefore a trivial solution.

Some tricky formal manipulations (combination, derivation, integration, substitution) of the weakly dispersive fully nonlinear approximate equations, allow to eliminate $\bar{u}(x)$; then we are led to study the following non linear autonomous differential equation:

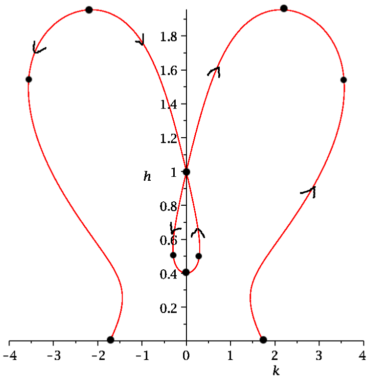
$$F_{a,b} := \frac{a}{3}h'^2 + 2\frac{bh}{(1+h'^2)^{\frac{1}{2}}} - a + (2a - 2b + 1)h - (a+2)h^2 + h^3.$$

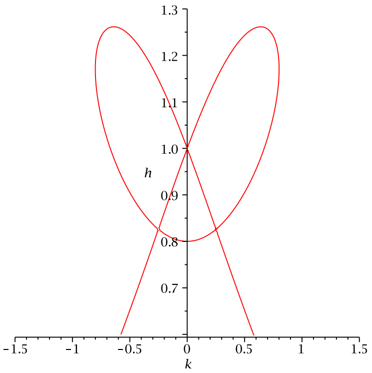
We are interested by the solutions which satisfy the following asymptotic condition, when x tends to plus or minus infinity

$$h(\infty) = 1, \ \ h'(\infty) = 0.$$

As a consequence, if $h(x)$ is a solution then $h(-x)$ is also a solution, and there are symmetrical waves, (as well as non symmetrical waves).

To discuss the number and behavior of the solutions of $F_{a,b}(h, h') = 0$ with respect to the pair $(a, b) \in [0, 2]^2$, a useful approach is to describe graphically the variations of h and h', studying the corresponding family of real algebraic curves $C_{a,b} \in \mathbf{R^2}$, with a certified topology. See e.g. [GVN]. The coordinates being k and h, we denote by $G_{a,b}$ the equation of $C_{a,b}$, deduced from $F_{a,b}(h, h')$ replacing h' by k.





1. Curves and discriminant

1.1. **Example.** The curve $C_{0.4,0.9}$, i.e. for the values $a = 0.4, b = 0.9$, is shown on the left of the figure. When k, representing the derivative h', is positive (resp. negative), h should increase (resp. decrease). So one can decompose the curve into parameterized and oriented branches. For that purpose, the points with an horizontal tangent or a multiple point, i.e. such that $diff(G_{a,b}, k) = 0$ need to be precised. In this first example, there are 4 such points: $A_2 := (0, 0.4), A_1 := (0, 1), A_3, A_4$, with approximately $A_3 = (2.1, 1.955)$ and $A_4 = (-2.1, 1.955)$. Call B_1 and B_2 the intersections of the curve with the k axis. Then, we get the following going up branches: from B_1 to A_3, from A_2 to A_1 (on the right side), from A_1 to A_3. And symmetrically the going down branches in the half plane $k < 0$.

Constrained by the asymptotic conditions, we consider cycles starting from (and arriving at) $(0, 1)$. In this example, the only continuous one is going down from A_1 to A_2 (on the left side), then going up from A_2 to A_1 (on the right side). Beside it, we can also consider discontinuous cycles such as the one going up from A_1 to A_3, then "jumping" from A_3 to A_4, then going down from A_4 to A_1. The first cycle will correspond to a true differentiable solution $h(x)$ of the differential equation, while the second cycle will correspond to a function $h(x)$ having a non differentiable point where the two (non zero) semi derivatives are opposite, hence create an angle. At such a point the two semi second derivatives are infinite, unfortunately this the conservation laws of the physical phenomenon. However, there are 4 points of the curve $C_{0.4,0.9}$ with a vertical tangent, they are approximately $V_1 = (0.3, 0.5), V_2 = (3.5, 1.5)$ and their symmetric, V_3, V_4, with respect to h axis; the two semi second derivatives at these points are zero. So, we can considera discontinuous cycle going down from A_1 to V_3 (on the left side), then going up from V_3 to A_1 (on the right side). It corresponds to an interesting new solitary (with an angle) which is physically possible.

We aim to analyze what happens when a and b vary.

1.2. **Local analysis when $k = 0$.** As noted in the example, the point on the h-axis are important; to determine them it suffices to substitute $k = 0$ and solve $G_{(a,b)}(h, 0) = 0$, which gives either $h = 1$ with multiplicity 2, or $h = a$. If there are two branches between these two points, they are necessarily symmetric, and we consider the loop starting from $k = 0, h = 1$ and going up (resp. down) to $k = 0, h = a$ if $a > 1$ (resp. $a < 1$). This will correspond to a crest (resp. a trough) solitary wave, above (resp. below) the constant solution $h = 1$.

Then, to investigate the local behavior at $(h = 1, k = 0)$, we compute the Taylor expansion of $G_{a,b}$ at that point. Up to order 3, we get:

$$3(a-1)(h-1)^2 - (a-3b)k^2 = 0.$$

Therefore, if $(a-1)(a-3b) < 0$ there is only an isolated point; if $(a-1)(a-3b) > 0$ then there is a double point corresponding of the crossing of two branches, i.e. no obstruction (at this local analysis) for the existence of a solitary wave. If $a = 1$, then we consider the Taylor expansion up to order 4: $(-1+3b)k^2 - 3(h-1)^3 + 3(h-1))bk^2 = 0$. Therefore if $b > \frac{1}{3}$, (resp. $b < \frac{1}{3}$) we get a cusp going up (resp. down); while if $b = \frac{1}{3}$, the Taylor expansion correspond to 3 lines including $h = 1$; i.e. no obstruction (at this local analysis) for the existence of a (non constant) solitary wave.

Now, the Taylor expansion of $G_{a,b}$ at the point $(h = a, k = 0)$, is equal to

$$3(a-1)^2(h-a) = a(3b-1)k^2$$

. So when $a \neq 1, b \neq \frac{1}{3}$ we get a usual point with an horizontal tangent, it is of convex type if $b > \frac{1}{3}$ and concave if $b < \frac{1}{3}$. Therefore if $a < 1,\ b > \frac{1}{3}$ or if $a > 1,\ b < \frac{1}{3}$, there is no obstruction (at this local analysis level) for the existence of a solitary wave. While if $a < 1,\ \frac{a}{3} < b < \frac{1}{3}$ or if $a > 1,\ \frac{a}{3} > b > \frac{1}{3}$, this local analysis only permits a solitary wave with an angle.

1.3. **Global analysis when $k \neq 0$.** For our global analysis and decomposition into branches, the points with horizontal tangents play a key role. They satisfy the two equations: $G_{a,b} = 0$ and $\frac{\partial G_{a,b}}{\partial k} = 0$. The second equation vanishes for $k = 0$ or for $a^2(k^2+1)^3 = 9b^2h^2$; from which we can express k^2 as a function in h and replace this expression in the first equation. So we get an equation depending only on h, but with a cube root operator. To get rid of it, and deal with polynomials, we introduce a new variable Y such that $h = \frac{a}{3b}Y^3$ and $k^2 = -1 + Y^2$, with $Y \geq 1$. Finally we are led to the following polynomial equation in Y:

$$f := a^2Y^9 + (-3a+2)abY^6 + (-18b^3 + 18ab^2 + 9b^2)Y^3 + 27Y^2b^3 - 36b^3.$$

The adapted tool to discuss the number of real roots of f depending on the pair (a, b), is the discriminant locus which is an algebraic curve in the $(a, b)-$plane, describing the point where f have multiple roots. here its implicit equation is a polynomial $D_1(a, b)$; this locus divides the plane into cells having the same number of real roots. However, we are only interested by real solutions $Y \geq 1$. Here, f admits $Y = 1$ as a solution if and only if $b = \frac{1}{3}$ or $a = 3b$ and in this last case $Y = 1$ is a double root (so it does not count for the transition between solutions bigger than 1 and smaller than 1). We deduce that some cells should be divided by the line $b = \frac{1}{3}$, or gathered across a branch of the discriminant locus (which corresponds to not interesting double roots, i.e. not real and bigger than 1). So, we will use a "real discriminant locus" to classify the global behaviors for the different values of (a, b).

In our setting, the discriminant polynomial D_1 factors into a square $(a-3b)^2$ and another polynomial $R(a, b)$ of degree 10 in (a, b).

It turns out that in the square $a \in [0, 2], b \in [0, 2]$, f admits 0 to 3 real solutions bigger than 1.

The line defined by the equation $(a - 3b) = 0$ is of special interest since it corresponds to a double root at a fixed value $Y = 1$, which corresponds to the double point at $h = 1$ and $k = 0$, and another simple solution $Y(b) \in [1, 2]$, increasing with b.

For the choice $a = 0.4, b = 0.9$ of Example 1, we find only one solution for Y hence only one solution for an extrema of h (beside the one corresponding to $k = 0$ that we got earlier in our analysis).

1.4. **Vertical tangents.** Once we have classified the curves thanks to their points with horizontal tangents, we need to locate the points with a vertical tangent, in order to predict potential solitary wave with an angle. We proceed similarly since they satisfy the equations $G_{a,b} = 0$ and $\frac{\partial G_{a,b}}{\partial h} = 0$. We introduce an auxiliary variable Z such that $k^2 = -1 + Z^2$, with $Z \geq 1$, and we get $a(Z^2 1) = 3(h-1)(2h^2 - h - 1$. Finally we are led to a polynomial equation in Z of degree 6; and we consider its discriminant $D_2(a, b)$. It turns out that D_2 factors into powers of a and of b, a polynomial of degree 5 in (a, b) and the same polynomial $R(a, b)$ which is a factor of D_1. This fact simplifies the case by case analysis.

2. Classification: One example by cell

Now, we can classify the different behaviors and detect solitary waves, just by seeing what happens when we choose a pair in each of the cells defined in the previous section. We also need to consider all the limit situations.

We point out the case where (a, b) belongs to the branch of the discriminant locus containing approximately $(a = 0.8, b = .3538557)$. It detects a special behavior: the corresponding solitary waves is differentiable but not twice differentiable in some special point; the curve $C_{0.8,0.3538557}$ is shown on the right of the figure.

References

[DCMM] D. Dutykh, D. Clamond, P. Milewsky and M. Mitsotakis. *An implicit-explicit finite volume scheme for fully nonlinear Serre equations.* Eur. J. App. Math. 24, 761-787. (2013).

[GVN] L. González-Vega and I. Necula: *Efficient topology determination of implicitly defined algebraic plane curves.* Computer Aided Geometric Design 19(9): 719-743, (2002).

[Serre] F. Serre *Contribution à l' étude des écoulements permanents et variables dans les canaux.* Houille Blanche 8, 374-388, (1953).

University of Nice and INRIA, France
E-mail address: galligo@unice.fr

LAMA, Université de Savoie, France
E-mail address: Denys.Dutykh@univ-savoie.fr

University of Nice, France
E-mail address: didier.clamond@gmail.com

A SIMILARITY TEST FOR ORE POLYNOMIALS

JOSÉ GÓMEZ-TORRECILLAS, F. J. LOBILLO, AND GABRIEL NAVARRO

ABSTRACT. Let R be an Ore extension of a division ring. Given Ore polynomials $f, g \in R$ of the same degree, a basic computational problem is to decide effectively whether f and g are similar, that is, if there exists an isomorphism of left R–modules between R/Rf and R/Rg. We show that if R is finite over its center C, then this problem can be reduced to check the existence of an isomorphism of C–modules.

INTRODUCTION

In 1933, O. Ore presented in [9] the foundations of non-commutative polynomials in one variable, defining what we call nowadays an Ore extension of a skew-field. He established the basic properties of these skew polynomials, including a factorization theory. The factorization was proved to be unique up to similarity of polynomials. In contrast with the commutative case, similar polynomials need not to be associated, and this entails that similar polynomials do not behave so well with respect to arithmetic than associated ones. For instance, products of pairwise similar polynomials are not necessarily similar.

Ore polynomials play a role in several branches of mathematics, from quantized algebras to differential operator rings. In 1976, Piret used skew polynomials over finite fields to introduce Cyclic Convolutional Codes, see [10], whose algebraic structure is deeply studied in [2]. This connection with Coding Theory suggests that new algorithms over skew polynomials should be developed. For instance, a Las Vegas factorization algorithm of skew polynomials over finite fields was proposed by Giesbrecht in [1].

In [4], we give a full proof of a generalization of [6, Ch. 3, Theorem 33] for finitely generated modules over a non-commutative PID finite over its center (Theorem 1.2). This theorem, in conjunction with the description from [8, Theorem 1.1.22] of the center of $D[X; \sigma]$ as a commutative polynomial ring, constitutes the key of our algorithm to decide if two given polynomials in $D[X; \sigma]$ are similar (see Subsection 2.1). Examples 2.2 and 2.5 and have been computed with the aid of mathematical software Sage [11].

1. THE ABSTRACT RESULT

In this section, R denotes a non-commutative principal ideal domain (PID, for short) in the sense of [6]. Every two-sided ideal I of R is then of the form $I = R\alpha = \alpha R$ for a suitable element $\alpha \in R$ (see [6, p. 37]). A left R–module M is *bounded* if its annihilator $Ann_R(M) = \{a \in R : am = 0 \ \forall m \in M\}$ is nonzero. In [6], Krull-Schmidt Theorem was applied to investigate the structure of any finitely generated bounded left R–module. With a little more work, the following structure theorem is deduced.

Proposition 1.1. *Let M be a finitely generated bounded left module over R. Let $\mathcal{P}(M)$ be the (finite) set of maximal two-sided ideals of R that contain $Ann_R(M)$. Then M admits a decomposition as a direct sum of submodules $M = \oplus_{P \in \mathcal{P}(M)} M_P$, where $M_P = \{m \in M : P^k m = 0\,\text{for some } k > 0\}$.*

Assume that R is *finite over its center C* (that is, R is free of finite rank as a C–module). If $f \in R$ is nonzero, then a straightforward application of the Cayley-Hamilton Theorem gives that f is a right factor of some nonzero element of C. Thus, $Rf \cap C \neq 0$ and, in particular, R/Rf is bounded left R–module, since $Rf \cap C \subseteq Ann_R(R/Rf)$. We deduce then that every left R–module of finite length is bounded. Let $f^* \in R$ be such that $Rf^* = f^*R = Ann_R(R/Rf)$ (the *bound* of f). The proof of [3, Lemma 3.6] runs here to prove that if R/Rf is a simple left R–module, then $C/(C \cap Rf^*)$ is a field and the simple Artinian ring R/Rf^* is a finite-dimensional algebra over $C/(C \cap Rf^*)$. Thus, in particular, R/Rf is a finite-dimensional $C/(C \cap Rf^*)$–vector space and, therefore, a C–module of finite length. Hence, every left R–module of finite length is a C–module of finite length, too. A finitely generated bounded left R–module M is said to be *centrally bounded* if every $P \in \mathcal{P}(M)$ is of the form $P = R\pi$, for some non-zero $\pi \in C$.

Theorem 1.2. *Let M, N be finitely generated and centrally bounded left R–modules. If R is finite over its center C, then $M \cong N$ as left R–modules if and only if $M \cong N$ as C–modules.*

In [4] we use Proposition 1.1 to reduce the proof of Theorem 1.2 to the case $M = M_P$ and $N = N_P$. Next, we show that the socle of M as a left R–module equals its socle as a C–module. This allows to prove first the theorem in the indecomposable case. Finally, using Krull-Schmidt decompositions, and the socle series of M and N, we complete the proof when the modules are decomposable.

2. The Algorithms

Consider an Ore extension $R = D[X;\sigma]$ of a division ring D by an automorphism σ of D (see, e.g. [8]). Assume that D is finite dimensional over its center $C(D)$, and that σ has finite order μ with respect to an inner automorphism associated to some $0 \neq u \in D$. By [8, Theorem 1.1.22] the center C of R is a polynomial ring over $K = C(D) \cap D^\sigma$, concretely $C = K[u^{-1}X^\mu]$. Here $D^\sigma = \{d \in D : \sigma(d) = d\}$. As a consequence, R is finite over C.

2.1. **Similarity of polynomials.** Two polynomials $f, g \in R$ are said to be *similar* if R/Rf and R/Rg are isomorphic as left R–modules. We say that $f \in R$ is X-torsionfree if f has non-zero term of degree zero. If $f, g \in R$ are X–torsionfree, then $M = R/Rf, N = R/Rg$ satisfy the hypotheses of Theorem 1.2. Now, if $f = f'X^r$ and $g = g'X^s$, with f', g' X–torsionfree, then f, g are similar if and only if $r = s$ and f' is similar to g'.

We thus get Algorithm 2.1 from Theorem 1.2. There, the basis $\mathcal{B}_1$ of R/Rf as a vector space over K is $\mathcal{B}_1 = \{u_i X^j : 0 \leq i < \rho,\ 0 \leq j < n\}$, and it is ordered lexicographically with $u_i < X$. Each equivalence class $u_i X^j + Rf$ is identified with its representative $u_i X^j$.

Algorithm 2.1. **Input:** $f, g \in R = D[X;\sigma]$ and a basis $\{u_0, \ldots, u_{\rho-1}\}$ of D over K.
Output: `True` if f, g are similar or `False` otherwise.

```
(1) If $\deg f \neq \deg g$ then return False.
(2) Write $f = cf'X^r$ and $g = dg'X^s$ where $f', g'$ are monic and $X$-torsionfree.
(3) If $r \neq s$ then return False.
```

(4) Let $n = \deg f' = \deg g'$. Let $M_{f'}, M_{g'}$ be the $n\rho \times n\rho$ matrices having as $(i + \rho j)$-th row, for all $0 \le i \le \rho - 1, 0 \le j \le n - 1$, the coefficients with respect to $\mathcal{B}_1$ of the reminder of the left division of $u^{-1}X^{\mu}u_iX^j = u_iu^{-1}X^{\mu+j}$ by f' and g' respectively.

(5) If $M_{f'}, M_{g'}$ have the same rational form then return `True`, else return `False`.

Algorithm 2.1 is correct since the matrices constructed in step 4 are associated to the linear maps providing the C–module structures of R/Rf' and R/Rg' (see, e.g., [7, §3.10]).

Example 2.2. Let $\mathbb{H}$ be the Hamilton quaternions over the rationals, and $R = \mathbb{H}[X; \sigma]$, where σ is the inner automorphism defined by $u = 1 + i$. Consider

$$\begin{aligned} f_1 &= x^2 + \left(-\tfrac{4}{3} + \tfrac{9}{7}i - \tfrac{25}{21}j + \tfrac{19}{21}k\right)x - \tfrac{10}{7}i - \tfrac{12}{7}j - \tfrac{6}{7}k, \\ f_2 &= x^2 + \left(\tfrac{2}{7} - \tfrac{1}{3}i - \tfrac{19}{21}j + \tfrac{25}{21}k\right)x + \tfrac{22}{21} + \tfrac{4}{21}i + \tfrac{38}{21}j - \tfrac{8}{7}k, \\ f_3 &= x^2 + (-i + 10j - k)\,x + \tfrac{7}{4}j. \end{aligned}$$

Algorithm 2.1 says that f_1 and f_2 are similar, but they are not similar to f_3.

If $D = \mathbb{F}$ is a finite field, then Algorithm 2.1 can be improved. By [8, Theorem 1.1.22], $C = K[X^{\mu}]$ is the center of R , where μ is the order of σ . Since K commutes with X and $\mathbb{F}$ commutes with X^{μ}, it follows that $S = K[X]$ and $T = \mathbb{F}[X^{\mu}]$ are commutative subrings of R, and $C \subseteq S, T \subseteq R$. As a consequence of Theorem 1.2, we have:

Corollary 2.3. *Let $f, g \in R$ be X-torsionfree. Then f and g are similar if and only if R/Rf and R/Rg are isomorphic as modules over C, S or T.*

So, in order to check if two given polynomials in R are similar, we can replace C by S or T in Algorithm 2.1. In the last case, an $\mathbb{F}$-basis of R/Rf, where $f \in R$ is a monic polynomial of degree n, is $\mathcal{B}_2 = \{1, X, \dots, X^{n-1}\}$. Hence we get:

Algorithm 2.4. Input: $f, g \in R = \mathbb{F}[X; \sigma]$.

Output: `True` if f, g are similar or `False` otherwise.

(1) If $\deg f \neq \deg g$ then return `False`.

(2) Write $f = cf'X^r$ and $g = dg'X^s$ where f', g' are monic and X-torsionfree.

(3) If $r \neq s$ then return `False`.

(4) Let $n = \deg f' = \deg g'$. Let $M_{f'}, M_{g'}$ be the $n \times n$ matrices having as i-th row, for all $0 \le i \le n - 1$, the coefficients with respect to $\mathcal{B}_2$ of the reminder of the left division of $X^{\mu+i}$ by f' and g' respectively.

(5) If $M_{f'}, M_{g'}$ have the same rational form then return `True`, else return `False`.

Example 2.5. Let $\mathbb{F}_{16}$ be generated over $\mathbb{F}_2$ by a with minimal polynomial $a^4 + a + 1$. Let $\sigma = \tau^2$, where τ is the Frobenius automorphism. Then the order of σ is $\mu = 2$. Let $f_1 = x^3 + a^{13}x^2 + ax + a^3$, $f_2 = x^3 + a^2x^2 + x + a^6$ and $f_3 = x^3 + a^8x^2 + a^3x + a^6$. Then the execution of Algorithm 2.4 leads to the matrices

$$M_{f_1} = \begin{pmatrix} 0 & 0 & 1 \\ a^3 & a & a^{13} \\ a^{10} & a^9 & a^8 \end{pmatrix}, \quad M_{f_2} = \begin{pmatrix} 0 & 0 & 1 \\ a^6 & 1 & a^2 \\ a^{14} & a^{12} & a^5 \end{pmatrix}, \quad M_{f_3} = \begin{pmatrix} 0 & 0 & 1 \\ a^6 & a^3 & a^2 + 1 \\ a^8 & a^6 & a^3 \end{pmatrix}$$

whose rational forms are

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & a^5 \\ 0 & 1 & a^{10} \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & a^5 \\ 0 & 1 & a^{10} \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},$$

respectively. Hence f_1 and f_2 are similar, but they are not similar to f_3.

Suppose matrix multiplication is performed in $\mathcal{O}(n^\omega)$ basic operations over its base field, with $\omega \geq 2$. Then the cost of step (5) in Algorithm 2.4 with respect to the basic arithmetic in K is $\mathcal{O}(n^\omega \mu \log(n+\mu)\log(\log n + \log \mu))$, whilst step (5) in Algorithm 2.1 needs $\mathcal{O}((n\mu)^\omega \log(n\mu)\log\log(n\mu))$ over K.

2.2. **An isomorphism test for finitely generated modules.** Let $M = R^m/L$ be a finitely generated left R–module, where L is a submodule of a free left R–module R^m. As detailed in [5, Section 2.5], by using the left and the right Euclidean Division Algorithms for R it is possible to find $f_1, \dots, f_k \in R$ of positive degree such that $M \cong R^a \oplus R/Rf_1 \oplus \cdots \oplus R/Rf_k$. For each $i = 1, \dots, k$, let us write $f_i = \overline{f}_i X^{m_i}$ with $m_i \geq 0$ and $\overline{f}_i$ are X–torsionfree. Since $R/Rf_i \cong R/RX^{m_i} \oplus R/R\overline{f}_i$, it follows that

$$M \cong R^a \oplus R/RX^{e_1} \oplus \cdots \oplus R/RX^{e_p} \oplus R/R\overline{f}_1 \oplus \cdots \oplus R/R\overline{f}_k, \tag{1}$$

where $a \geq 0$ and $0 < e_1 \leq \cdots \leq e_p$ are integers, and $\overline{f}_1, \dots, \overline{f}_k \in R$ are X–torsionfree nonconstant polynomials. We say that (1) M is a *rough decomposition* of M.

Theorem 2.6. *Let M and N be finitely generated left R–modules, and assume that* (1) *is a rough decomposition of M, and let*

$$R^{a'} \oplus R/RX^{e'_1} \oplus \cdots \oplus R/RX^{{e'}_{p'}} \oplus R/R\overline{g}_1 \oplus \cdots \oplus R/R\overline{g}_{q'}$$

be a rough decomposition of N. Then M and N are isomorphic as left R–modules if and only if $a = a'$, $p = p'$, $e_i = e'_i$ for $i = 1, \dots, p$ and $R/R\overline{f}_1 \oplus \cdots \oplus R/R\overline{f}_q \cong R/R\overline{g}_1 \oplus \cdots \oplus R/R\overline{g}_{q'}$ as modules over the center C of R.

As a consequence, similar algorithms to Algorithms 2.1 and 2.4 can be provided.

References

1. M. Giesbrecht, *Factoring in skew-polynomial rings over finite fields*, J. Symb. Comp. **26** (1998), 463–486.
2. H. Gluesing-Luerssen, W. Schmale, *On cyclic convolutional codes*, Acta Appl. Math. **82** (2004), 183–237.
3. J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, *Computing the bound of an Ore polynomial. Applications to factorization*, 2013. Available at http://arxiv.org/abs/1307.5529
4. J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, *On isomorphisms of modules over non-commutative PID*, accepted in ISSAC 2014.
5. J. Gómez-Torrecillas, *Basic Module Theory over Non-commutative Rings with Computational Aspects of Operator Algebras*, in: Algebraic and Algorithmic Aspects of Differential and Integral Operators (M. Barkatou, et al. eds.), Lect. Notes in Comput. Sci., vol. 8372, pp. 23–82, Springer, 2014.
6. N. Jacobson, *The Theory of Rings*, Mathematical Surveys, no. II, American Mathematical Society, 1943.
7. ———, *Basic Algebra*, second ed., vol. I, W. H. Freeman and Co, 1985.
8. ———, *Finite-dimensional division algebras over fields.*, Berlin: Springer, 1996.
9. O. Ore, *Theory of non-commutative polynomials*, Annals of Mathematics **34** (1933), no. 3, pp. 480–508.
10. P. Piret, *Structure and constructions of cyclic convolutional codes*, IEEE Transactions on Information Theory **22** (1976), no. 2, 147–155.
11. W. A. Stein et al., *Sage Mathematics Software (Version 5.12)*, The Sage Development Team, 2014, http://www.sagemath.org

Universidad de Granada
E-mail address: gomezj@ugr.es, jlobillo@ugr.es, gnavarro@ugr.es

RADICALS OF ORE POLYNOMIALS

MAXIMILIAN JAROSCHEK

ABSTRACT. We give a comprehensible algorithm to compute the radical of an Ore operator. Given an operator P, we find another operator L and a positive integer k such that $P = L^k$ and k is maximal among all integers for which such an operator L exists.

1. INTRODUCTION

The problem of factoring commutative univariate polynomials with the help of a computer is a classical and still active field of research. Frequently utilized algorithms are based on the work of Cantor-Zassenhaus [4], Berlekamp [2], Kaltofen [5] and van Hoeij [10]. An important preprocessing step for many of these algorithms is to compute the squarefree decomposition of the input polynomial, i.e. given a polynomial $p \in \mathbb{K}[x]$, find $g_1, \dots, g_m \in \mathbb{K}[x]$ with $\gcd(g_i, g_j) = \gcd(g_i, g_i') = 1$ such that

$$p = g_1 g_2^2 \cdots g_m^m.$$

In the noncommutative setting, simplifying the process of factoring Ore polynomials by identifying repeated factors is not yet available for the existing factoring algorithms like [3, 8]. As a first step towards such a preprocessing method we present an algorithmic solution to the following problem:

Given an Ore operator P, i.e. an element of an Ore algebra $\mathbb{K}[y][X; \sigma, \delta]$, find another operator $L \in \mathbb{K}[y][X; \sigma, \delta]$ and a positive integer k such that

$$P = L^k, \tag{1}$$

and k is maximal among all integers for which such an operator L exists. In the outline of the algorithm presented here, we only consider the shift case for sake of simplicity, i.e. we take Ore operators in the algebra $\mathbb{K}[y][X; \sigma, 0]$ with trivial pseudo-derivation $\delta = 0$. Remarks on the differential case with $P \in \mathbb{K}[y][X; 1, \delta]$ and the case of general Ore algebras are given in Section 4. For details on Ore algebras see [7].

Our algorithm is based on the solution of the corresponding problem in the commutative case and on (linear) algebra methods for determining suitable values for symbolic coefficients.

2. PRELIMINARIES

Let $\mathbb{K}$ be a computable field. We fix an operator P in the Ore algebra $\mathbb{K}[y][X; \sigma, 0]$. Operators are denoted by capital letters and the ith coefficient of an operator by the corresponding lower case letter with the index i. The order of an operator L is its degree with respect to X and is denoted by $\operatorname{ord}(L)$. By $\deg(L)$ we refer to the degree of L in y.

Author supported by Technologietransfer 2013/14 des Landes Oberösterreich.

3. The algorithm

3.1. **Degenerate Cases.** In this section we cover the cases where either $\operatorname{ord}(P) = 0$ or $\deg(P) = 0$. In both cases, we can assume $P \in \mathbb{K}[x]$, i.e. we work in a commutative domain. We compute the squarefree decomposition $g_1, \ldots, g_m$ of p (e.g. by Yun's algorithm [11]) and the greatest common divisor k of all the elements in the set $\{i \in \mathbb{N}^* \mid \deg(g_i) > 0\}$. Then it is easy to see that k is as required and L is given by

$$L = \operatorname{lc}(P)^{1/k} g_1^{1/k} g_2^{2/k} \ldots g_m^{m/k}.$$

Now we establish how to solve this problem for shift operators by solving a linear and an algebraic system of equations.

3.2. **Main Idea.** For the noncommutative case, we don't have a squarefree decomposition to simplify the task. We exploit noncommutativity to solve the problem:

Observe that for P and L as above we have that

$$PL = L^k L = L^{k+1} = LL^k = LP.$$

Therefore, L is a solution to the equation

$$PL - LP = 0. \tag{2}$$

This means that L is an element of the centralizer of P.

Definition 3.1. Let $r, d \in \mathbb{N}$. We call the set

$$\mathcal{C}_{r,d}(P) = \{L \in \mathbb{K}[y][X; \sigma, 0] \mid PL = LP, \operatorname{ord}(L) \leq r, \deg(L) \leq d\},$$

the centralizer of P (with order r and degree d).

The centralizer of P with order r and degree d is a $\mathbb{K}$-vector space. In order to find L as in (1), we compute a basis of $\mathcal{C}_{r,d}(P)$ for certain $r, d \in \mathbb{N}$ and then construct L as a linear combination of the basis elements.

The outline of our algorithm is as follows.

```
Algorithm 3.1: OreRadical
  Input:  An operator $P \in \mathbb{K}[y][X; \sigma, 0]$ with
            $\operatorname{ord}(P) \cdot \deg(P) \neq 0$.
  Output: An operator $L$ and an integer $k$ such that $P = L^k$
            and $k$ is maximal among all integers for which such
            an operator $L$ exists.
  1. If $\operatorname{ord}(P) = 0$ or $\deg(P) = 0$: solve as in the
       commutative case.
  2. Compute candidates for $k$.
  3. For each candidate $k'$, do:
  4.       Compute a basis for $\mathcal{C}_{\operatorname{ord}(P)/k', \deg(P)/k'}(P)$.
  5.       If it exists, compute an element $L_{k'}$ in $\mathcal{C}_{r,d}(P)$ for which
             $P = (L_{k'})^{k'}$ holds.
  6. Return $(L_k, k)$ such that $k$ is maximal.
```

We already have seen in Section 3.1 how to carry out step **1**. We now show in detail how to carry out the steps **2** – **5**.

3.3. **Candidates for the Exponent.** If $P = L^k$ holds, then also $p_0 = l_0^k$ has to hold. Therefore it suffices to look for a candidate for k in the commutative case. If $g_1, \ldots, g_m$ are the factors in the squarefree decomposition of p_0, we see that the exponent k has to divide each index i for which g_i in the squarefree decomposition $g_1^1 g_2^2 \ldots g_m^m$ is not equal to 1 and it also has to divide $\operatorname{ord}(P)$ and $\deg(P)$ since we have that

$$\operatorname{ord}(P) = k \cdot \operatorname{ord}(L) \text{ and } \deg(P) = k \cdot \deg(L).$$

Therefore the set of candidates is given by the set of all common divisors of $\operatorname{ord}(P)$, $\deg(P)$ and of the indices i for which $g_i \neq 1$.

3.4. **Looping Through the Candidates.** It is clear that the real k has to be contained in the set of candidates computed in Section 3.3. The choice on the order in which the candidates are considered in the for loop of the algorithm will affect its running time. One way is to begin with the smallest $k' \neq 1$. This will guarantee that we find a nontrivial solution on the first try (if one exists), but it might be of the form $L^{k'}$ where $k' < k$, e.g. $P = L^4$ and we choose $k' = 2$. The algorithm then has to be applied recursively. On the other hand, we can start with the largest candidate and be guaranteed to find L without a recursive call, but it might be necessary to try several different candidates, e.g. when $P = L^2$ and $l_0 = n^2$ we would choose $k' = 4$. Depending on the input, one strategy may be better than the other, but in general it is not clear a priori which method is preferable.

3.5. **Computing a Basis for the Centralizer.** Having chosen a candidate k', we now have to look for $L_{k'}$ in $\mathcal{C} := \mathcal{C}_{\operatorname{ord}(P)/k', \deg(P)/k'}(P)$. We compute a basis for $\mathcal{C}$ by letting A be an operator in $\mathbb{K}[y][X;\sigma,0]$ of order $\operatorname{ord}(P)/k'$ and degree $\deg(P)/k'$ with undetermined coefficients. Setting $AP - PA$ equal to zero then gives a linear system of equations by coefficient comparison. A basis for the solution space of this system is a basis for $\mathcal{C}$.

3.6. **Finding the Radical in the Centralizer.** A basis of the solution space of $\mathcal{C}$ corresponds to an ordered set of operators

$$(B_1, \ldots, B_\ell, 1),$$

with $B_i > B_{i+1} > 1$ for $1 \leq i < \ell$ with respect to the lexicographic term ordering for which $y < X$. Let $c_1, \ldots, c_{\ell+1}$ be undetermined and consider the equation

$$\underbrace{(c_1 B_1 + c_2 B_2 + \cdots + c_\ell B_\ell + c_{\ell+1})}_{=:L_{k'}}{}^{\operatorname{ord}(P)/k'} - P = 0. \tag{3}$$

Again, by coefficient comparison, this gives a system of algebraic equations. If there exists a solution, the special form of the system allows us to find it without the help of Gröbner bases. By construction, the operator on the left hand side of (3) contains a coefficient that only depends on c_1, a coefficient that only depends on c_1 and c_2 and so on. Thus we can determine the c_i's one after another. If we find a solution for all the c_i's, we can construct $L_{k'}$. If we don't find a solution, we have to consider the next candidate for k. If P cannot be written as the power of another operator, the algorithm will eventually return $L = P$ and $k = 1$.

4. Generalizations and Future Work

The algorithm can be easily adapted to work with other Ore algebras. The only time we make use of the fact that we are working in the shift algebra is in Section 3.3. For differential operators in $\mathbb{K}[y][X;1,\delta]$, the equation $p_0 = l_0^k$ does not necessarily hold, but in this case we can replace it with $\mathrm{lc}(P) = \mathrm{lc}(L)^k$, the analogous relation for the leading coefficients of P and L.

For an Ore algebra $\mathbb{K}[y][X;\sigma,\delta]$ with nontrivial σ and δ it is well known that there exists a computable isomorphism ϕ from $\mathbb{K}(y)[X;\sigma,\delta]$ to the algebra $\mathbb{K}(y)[X;\sigma,0]$ with trivial pseudo-derivation [1]. Starting with $P \in \mathbb{K}[y][X;\sigma,\delta]$, it might happen that $\phi(P)$ has rational function coefficients. The trailing coefficient of P then is of the form r^k where r is a rational function in $\mathbb{K}(y)$ and both, the numerator and the denominator of r^k can be used to find candidates for k as in Section 3.3. Once the candidates have been determined, the rest of the algorithm can be carried out with $P \in \mathbb{K}[y][X;\sigma,\delta]$ instead of $\phi(P) \in \mathbb{K}(y)[X;\sigma,0]$.

For the shift and the differential case, the algorithm was implemented in Sage [9] and will be included in the next release of the Ore algebra package [6].

The result presented here is only a first step in simplifying the task of factoring Ore polynomials. As a next goal, we would like to be able to detect if an operator is of the form $P = AL^k$ and compute its “right squarefree part” $\mathrm{rsqfp}(P) := AL$.

References

[1] S. A. Abramov, H. Q. Le, and Z. Li. Univariate Ore polynomial rings in computer algebra. *Journal of Mathematical Sciences*, 131(5):5885–5903, 2005.

[2] Elwyn R Berlekamp. Factoring polynomials over finite fields. *Bell System Technical Journal*, 46(8):1853–1859, 1967.

[3] M. Bronstein and M. Petkovšek. An introduction to pseudo-linear algebra. *Theoretical Computer Science*, 157:3–33, 1996.

[4] David G. Cantor and Hans Zassenhaus. A new algorithm for factoring polynomials over finite fields. *Mathematics of Computation*, 36(154):pp. 587–592, 1981.

[5] Erich Kaltofen and Victor Shoup. Subquadratic-time factoring of polynomials over finite fields. In *Math. Comp*, pages 398–406, 1998.

[6] M. Kauers, M. Jaroschek, and F. Johansson. *Ore algebra package for Sage*, 2013. `https://www.risc.jku.at`.

[7] Ø. Ore. Theory of non-commutative polynomials. *Annals of Mathematics*, 34(3):480–508, 1933.

[8] M. Petkovšek. Hypergeometric solutions of linear recurrences with polynomial coefficients. *Journal of Symbolic Computation*, 14(2–3):243 – 264, 1992.

[9] W. A. Stein et al. *Sage Mathematics Software (Version 6.1.1)*. The Sage Development Team, 2014. `http://www.sagemath.org`.

[10] Mark van Hoeij. Factoring polynomials and the knapsack problem. *J. Number Theory*, 95(2):167–189, 2002.

[11] David Y.Y. Yun. On square-free decomposition algorithms. In *Proceedings of the Third ACM Symposium on Symbolic and Algebraic Computation*, SYMSAC ’76, pages 26–35, New York, NY, USA, 1976. ACM.

Research Institute for Symbolic Computation, Johannes Kepler University, Linz, Austria
E-mail address: `mjarosch@risc.jku.at`

ALGORITHMS FOR COMPUTATION OF TRANSCENDENTAL FUNCTIONS WITH NEAR TO OPTIMAL COMPLEXITY

EKATHERINA A. KARATSUBA

The calculation of the values of a function with a given accuracy in an appropriate time of computer work is one of the central problems in computational mathematics. The first nontrivial problem of such kind stated by A.N. Kolmogorov (see [29], [15], [16]) in the end of 50-s was the problem of the study of the complexity $M(n)$ of computation of the product of two n -digit integers. A solution was found in 1960 by Kolmogorov's student A.A. Karatsuba (see [13]–[16], see also [27], [28]) who invented the first fast method, method of fast multiplication.

From the moment of the discovery of ”fast multiplication”, different fast algorithms were constructed (e.g. the Schönhage-Strassen multiplication, see [31], [32]; the FFT, see [11]; fast matrix multiplication, see [34], [32]; the AGM, see [6], [8], etc.) and were implemented in the soft- and sometimes in the hardware. We give an overview of existing fast algorithms (see [1]–[5], [10]–[12], [31]–[32], [35]), especially for the computation of transcendental functions (see [7]–[10], [16]–[27], [30]).

We present a general method for fast evaluation of the functions of type of the Siegel E -function (see [33]), the so-called FEE method, constructed by the author (see [17]–[27]), and some other fast algorithms developed for computation of both elementary transcendental functions and higher transcendental functions.

By means of the FEE it's possible to calculate the following series:

$$f_1 = f_1(z) = \sum_{j=0}^{\infty} \frac{a(j)}{b(j)} z^j, \tag{1}$$

$$f_2 = f_2(z) = \sum_{j=0}^{\infty} \frac{a(j)}{b(j)} \frac{z^j}{j!}, \tag{2}$$

assuming that $a(j)$, $b(j)$ are integers, $|a(j)| + |b(j)| \leq (Cj)^K$; $|z| \ < \ 1$; K and C are constants, and z is an algebraic number, with the complexity bounds

$$s_{f_1}(n) = O\left(M(n)\log^2 n\right),$$
$$s_{f_2}(n) = O\left(M(n)\log n\right).$$

Here $M(n)$ is the algorithmic complexity of a multiplication algorithm such that $M(n) < n^{1+\varepsilon}$, for any $\varepsilon > 0$ and $n > n_1(\varepsilon)$, that corresponds to the $M(n)$ from A.A. Karatsuba's "linear" algorithm (see [16], [27]), or from Schönhage-Strassen's algorithm (see [31], [32]), or from Fürer's algorithm (see [12]).

The method FEE is the method of fast summation of the series of a special form, including the series of the form (1), (2). The FEE permits to compute any elementary transcendental function for any value of the argument, the classical constants e, π, the Euler constant γ, the Catalan and the Apery constants, such higher transcendental functions as the Euler gamma function and it's derivatives, the hypergeometric, spherical, cylindrical and other functions for algebraic values of the argument and parameters, the Riemann zeta function for integer values of the argument and the Hurwitz zeta function for integer argument and algebraic values of the parameter, and also such special integrals as the integral of probability, the Fresnel integrals, the integral exponential function, the integral sine and cosine, and some other integrals for algebraic values of the argument with the complexity bound which is close to the optimal one, namely

$$s_f(n) = O\left(n \log^3 n \log\log n\right).$$

At present, the FEE only makes it possible to calculate fast the values of the functions from the class of higher transcendental functions, certain special integrals of mathematical physics and such classical constants as Euler's, Catalan's and Apery's constants. An additional advantage of the method FEE is the possibility of parallelizing the algorithms based on the FEE.

Recently author found new formulas for representation of certain number-theoretic constants. These are fast approximations providing a possibility to construct algorithms for evaluation some of these constants with the computational complexity which is close to optimal one.

Theorem 1. *The following approximation to the Catalan constant G is valid:*

$$G = \frac{1}{4}\sum_{n=1}^{\infty} \frac{8^{n-1}((n-1)!)^3}{(2n-1)!!}\left(\frac{6n-3}{((4n-3)!!!!)^2} - \frac{6n-1}{((4n-1)!!!!)^2}\right). \tag{3}$$

By using (3), one can construct the FEE algorithm for calculation of G with the complexity bound

$$s_G(n) = \left(O(M(n)\log^2 n\right) = O\left(n\log^3 n \log\log n\right).$$

Theorem 2. *The following approximation to the Riemann zeta function value $\zeta(2)$ is valid:*

$$\zeta(2) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{\binom{2n}{n}n^2}\frac{10n-3}{4n-2} = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{\binom{2n}{n}n^2}\left(\frac{5}{2} + \frac{1}{2n-1}\right). \tag{4}$$

By using (4), one can construct the FEE algorithms for calculation both $\zeta(2)$ and the classical constant π with the complexity bounds

$$s_{\zeta(2)}(n) = \left(O(M(n)\log^2 n\right), \quad s_\pi(n) = \left(O(M(n)\log^2 n\right).$$

We discuss the ways of the further development of the field of fast algorithms and formulate certain open problems from the field of algorithmic complexity.

REFERENCES

[1] V. B. Alekseev, *From the Karatsuba Method for Fast Multiplication of Numbers to Fast Algorithms for Discrete Functions.* Proceddings of the Steklov Inst.of Math., Vol. 218. pp. 15–22 (1997).

[2] E. Bach, *The complexity of number-theoretic constants.* Info.Proc.Letters, Vol. 62, pp. 145–152 (1997).

[3] D. H. Bailey, P. B. Borwein and S. Plouffe, *On the rapid computation of various polylogarithmic constants.* Math. Comp., Vol. 66, pp. 903–913 (1997).

[4] Bailey D. H., Borwein J. M., Mattingly A., Wightwick G., *The computation of previously inaccessible digits of* π^2 *and Catalan's constant*, Notices of AMS, Vol. 50, pp. 844–854 (2013).

[5] Yu. V. Benderskij, *Fast Computations.* Dokl. Akad. Nauk SSSR, Vol. 223, No 5, pp. 1041–1043 (1975).

[6] J. M. Borwein and P. B. Borwein, *Pi and the AGM.* Wiley, 414 pp., New York (1987).

[7] J. M. Borwein, D. M. Bradley and R. E. Crandall, *Computational strategies for the Riemann zeta function.* J. of Comput. Appl. Math., Vol. 121 , No 1-2 , pp. 247–296 (2000).

[8] R. P. Brent, *Fast Multiple-Precision Evaluation of Elementary Functions.* ACM, Vol. 23, No 2, pp. 242–251 (1976).

[9] R. P. Brent and E. M. McMillan, *Some new algorithms for high-precision computation of Euler's constant.* Math. Comp., Vol. 34, pp. 305–312 (1980).

[10] S. A. Cook, *On the minimum computation time of functions.* Thesis, Harvard University (1966).

[11] J. W. Cooley and J. W. Tukey, *An algorithm for the machine calculation of complex Fourier series.* Math. Comp., Vol. 19, pp. 297–301 (1965).

[12] Fürer M., *Faster integer multiplication.* SIAM Journal Computing, Vol. 39, No 3, pp. 979–1005 (2009).

[13] Karatsuba A., Ofman Yu., *Multiplication of multidigit numbers on automata.* Soviet Physics-Doklady, Vol. 7, pp. 595–596 (1963); translation from Dokl. Akad. Nauk SSSR, Vol.145, No 2, pp. 293–294 (1962).

[14] Karacuba A., *Berechnungen und die Kompliziertheit von Beziehungen.* EIK, Vol. 11, pp. 10–12 (1975).

[15] A. A. Karatsuba, *The complexity of computations.* Proc. Steklov Inst. Math., Vol. 211, pp. 169–183 (1995); translation from Trudy Mat. Inst. Steklova, Vol. 211, pp. 186–202 (1995).

[16] A. A. Karatsuba, *Comments to My Works, Written by Myself.* Proc. Steklov Inst. Math., Vol. 282 suppl. 1, pp. 1–23 (2013).

[17] E. A. Karatsuba, *Fast computation of $exp(x)$* . Problems of Information Transmission, Vol. 26, No 3, p. 109, Chronicle-17th All-Union School on Theory of Information and its Applications (1990).

[18] E. A. Karatsuba, *On a new method for fast evaluation of transcendental functions.* Russ. Math. Surv., Vol. 46, No. 2, pp. 246–247 (1991); translation from Usp. Mat. Nauk, Vol. 46, No. 2(278), pp.219–220 (1991).

[19] E. A. Karatsuba, *Fast evaluations of transcendental functions.* Probl. Inf. Transm., Vol. 27, No. 4, pp. 339–360 (1991); translation from Probl. Peredachi Inf., Vol. 27, No. 4, pp. 87-=110 (1991).

[20] E. A. Karatsuba, *Fast evaluation of $\zeta(3)$* , Probl. Inf. Transm., Vol .29, No. 1, pp. 58–62 (1993); translation from Probl. Peredachi Inf., Vol. 29, No.1, pp.68–73 (1993).

[21] Catherine A.Karatsuba, *Fast evaluation of Bessel functions.* Integral Transforms and Special Functions, Vol.1, No 4, pp. 269–276 (1993).

[22] E. A. Karatsuba, *Fast Evaluation of Riemann zeta-function $\zeta(s)$ for integer values of argument s.* Probl. Inf. Transm., Vol. 31, No. 4, pp. 353–362 (1995); translation from Probl. Peredachi Inf., Vol. 31, No. 4, pp. 69–80 (1995).

[23] E. A. Karatsuba, *On fast computation of Riemann zeta-function for integer values of argument.* Dokl. Math., Vol. 54, No.1, p. 626 (1996); translation from Dokl. Akad. Nauk, Ross. Akad. Nauk, Vol. 349, No.4, p. 463 (1996).

[24] E. A. Karatsuba, *Fast evaluation of Hurwitz zeta function and Dirichlet L-series.* Probl. Inf. Transm., Vol. 34, No. 4, pp. 342–353 (1998); translation from Probl. Peredachi. Inf., Vol. 34, No. 4, pp. 62–75 (1998).

[25] Ekatharine A. Karatsuba, *Fast evaluation of hypergeometric function by FEE.* Computational Methods and Function Theory (CMFT'97), N. Papamichael, St. Ruscheweyh and E.B. Saff, eds., World Sc.Pub., pp. 303–314 (1999).

[26] E. A. Karatsuba, *Fast computation of $\zeta(3)$ and of some special integrals, using the polylogarithms, the Ramanujan formula and it's generalization.* J. of Numerical Mathematics BIT, Vol. 41, No 4, pp. 722–730 (2001).

[27] E. A. Karatsuba, *Fast Catalan constant calculating via the approximations reached by transformations of Kummer's type.* Discrete Mathematics and Applications (2014); translation from Discrete Mathematics, Vol. 25, No 4 , pp. 74–87 (2013).

[28] D. E. Knuth, *The art of computer programming.* v.2 Addison-Wesley Publ.Co., 724 pp., Reading (1969).

[29] A. N. Kolmogorov, *Information Theory and the Theory of Algorithms.* Publ. Nauka, 303 pp., Moscow (1987).

[30] D. W. Lozier and F. W. J. Olver, *Numerical Evaluation of Special Functions.* Mathematics of Computation 1943-1993: A Half -Century of Computational Mathematics, W. Gautschi,eds., Proc. Sympos. Applied Mathematics, AMS, Vol. 48, pp. 79–125 (1994).

[31] A. Schönhage und V. Strassen, *Schnelle Multiplikation großer Zahlen.* Comput., Vol. 7, pp. 281–292 (1971).

[32] A. Schönhage, A. F. W. Grotefeld and E. Vetter, *Fast Algorithms.* BI-Wiss.-Verl., 300 pp., Zürich (1994).

[33] C. L. Siegel, *Transcendental numbers.* Princeton University Press, 102 pp., Princeton (1949).

[34] V. Strassen, *Gaussian elimination is not optimal.* J. Numer. Math., Vol. 13, pp. 354–356 (1969).

[35] A. L. Toom, *The complexity of a scheme of functional elements realising the multiplication of integers.* Dokl.Akad.Nauk SSSR, Vol. 150, No 3, pp. 496–498 (1963).

Dorodnicyn Computing Centre of RAS, Vavilova 40, Moscow, 119333 RUSSIA
E-mail address: ekar@ccas.ru

ZIGZAG HOMOLOGY FOR BIOMEDICAL IMAGE PROCESSING

GADEA MATA, MIGUEL MORALES, ANA ROMERO, AND JULIO RUBIO

ABSTRACT. We explain how the problem of distinguishing among different features in a stack of images can be approached by means of zigzag homology. The idea is then applied to neuronal images, allowing us to identify different dendrites which would appear mixed in the maximal projection image. The algorithm has been implemented as a plugin in the Fiji/ImageJ framework. Some results from actual neuronal images are presented.

INTRODUCTION

The project *SpineUP* (`http://www.spineup.es`) is a joint venture of a Computer Science group at Universidad de La Rioja and a biologists team, led by M. Morales. One of the objectives of the program is to produce software systems to automate some of the (boring and time consuming) tasks needed to process neuronal images got from microscopical devices. These efforts have given rise to a number of plugins in the Fiji/ImageJ framework, which are currently in use in several laboratories (see [RHM$^+$14] for a gentle general presentation).

Once a picture is taken, one of the most important steps is to distinguish the *object of interest* in the image, from the *noise* included in it. In our case, the object of interest can be, for instance, a sole neuron or a sole dendrite in a neuron. Related to this aim, in [HMC$^+$13] an algorithm was presented to mark in the maximal projection (a digest of the contents of a *stack* of images) the dendrites of a neuron (discarding both spurious noise and dendrites coming from other neurons). The routine has an interpretation in terms of *persistent homology* but had the drawback of being incapable of recognizing dendrites crossing in different heights, and unavoidably mixed in the maximal projection.

Here, we move from persistent homology to zigzag homology, another tool from Computational Topology, allowing us to overcome the mentioned drawback, and opening the way to a 3D-reconstruction of a neuron.

1. ZIGZAG PERSISTENCE FOR $3D$ IMAGE RECONSTRUCTION

The theory of zigzag persistence [CdS10] provides an extension of persistent homology [ZC05] to diagrams of topological spaces of the form:

$$X_1 \leftrightarrow X_2 \leftrightarrow \cdots \leftrightarrow X_m$$

where the arrows can point either left or right.

For each $n \in \mathbb{N}$, the sequence of vector spaces and linear maps:

$$H_n(X_1) \leftrightarrow H_n(X_2) \leftrightarrow \cdots \leftrightarrow H_n(X_m)$$

is called a *zigzag module*. In [CdS10] it is shown that such sequences have the structure of an abelian category and can be classified up to isomorphism by a multi-set of intervals $\{[a_i, b_i]\}$ with $1 \leq a_i \leq b_i \leq m$ and therefore can be represented by means of a *barcode diagram*.

Let us consider now $S_1, \dots, S_n$ to be the different slices of a Z-stack of images. Since these images do not usually define a filtration one cannot directly apply persistent homology techniques. However, in this work we show that zigzag persistence solves this problem and can be useful to detect the structure of different elements in the image in a $3D$-reconstruction process.

To this aim, we begin by producing the following sequence:

$$S_1 \hookrightarrow S_1 \sqcup S_2 \hookleftarrow S_2 \hookrightarrow S_2 \sqcup S_3 \hookleftarrow \cdots \hookrightarrow S_{m-1} \sqcup S_m \hookleftarrow S_m$$

where $S_i \sqcup S_{i+1}$ can denote (depending on the type of the image to be studied, see Section 2) the union of the slices S_i and S_{i+1} or the maximal projection of both slices.

One can observe that the zigzag homology of this sequence describes the continuity of homology classes between the different slices. In particular, we consider the zigzag module corresponding to 0-homology:

$$(1)\quad H_0(S_1) \to H_0(S_1 \sqcup S_2) \leftarrow H_0(S_2) \to H_0(S_2 \sqcup S_3) \leftarrow \cdots \to H_0(S_{m-1} \sqcup S_m) \leftarrow H_0(S_m)$$

Here one can observe that intervals in the barcode diagram starting at S_1 or at $S_i \sqcup S_{i+1}$ for some i and dying at S_m or at $S_j \sqcup S_{j+1}$ for some j correspond to the different connected components appearing in the $3D$ image. One can also observe that intervals starting at some S_i correspond to different connected components in S_i which merge in $S_{i-1} \sqcup S_i$. Similarly, intervals dying at some S_i represents components which merge with another one in $S_i \sqcup S_{i+1}$. In this way, the computation of zigzag homology of the previous module allows one to determine the different connected components in the $3D$ image.

In our particular case of brain images obtained by confocal microscopy, zigzag persistence can be used to detect the different neurons appearing in an image and discard non-relevant elements considered as noise. Neuron components correspond to *long* intervals in the barcode (that is, elements which *persist* along several slices), in contrast with noise which is present in few steps. Following zigzag persistence ideas, a plugin for ImageJ/Fiji [S$^+$12, Ras12] has been developed representing with different colors over the maximal projection the different (parts of) neurons appearing in the image. For practical reasons, some preprocessing steps have been applied to initial images $S_1, \dots, S_m$ to reduce noise by smoothing.

2. NEURONZIGZAGJ, A PLUGIN FOR NEURON DETECTION

The theory of zigzag persistence has been used to develop a plugin able to extract the neuronal structure and to identify two or more different neuronal dendrites from a stack of images. This application, called NeuronZigZagJ [Mat14], has been implemented as a plugin for ImageJ [Ras12].

In this work we have considered two different types of images, both of them acquired with a confocal microscopy. A first class of images represents a basal hippocampal rat neuron in culture transfected with an Actin-GFP vector; the second one shows a DiI staining of the basal dendritic segment of a mouse pyramidal hippocampal neuron (see Figure 1). These images are Z-stacks, which have about between 10 and 50 slices. These slices are different images in the Z-plane. For example, Figure 1 shows the maximal projection of a Z-stack that has 15 slices. For continuing the study, we have selected the part of the image which is inside the white rectangle. Figure 2 depicts each one of these 15 slices.

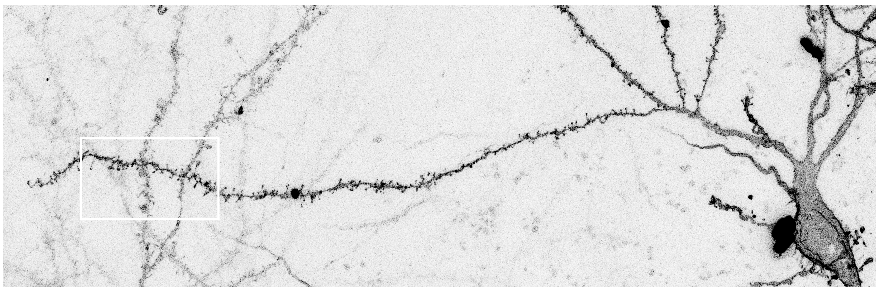


FIGURE 1. Basal dendritic segment of a mouse pyramidal hippocampal neuron obtained using DiI staining.

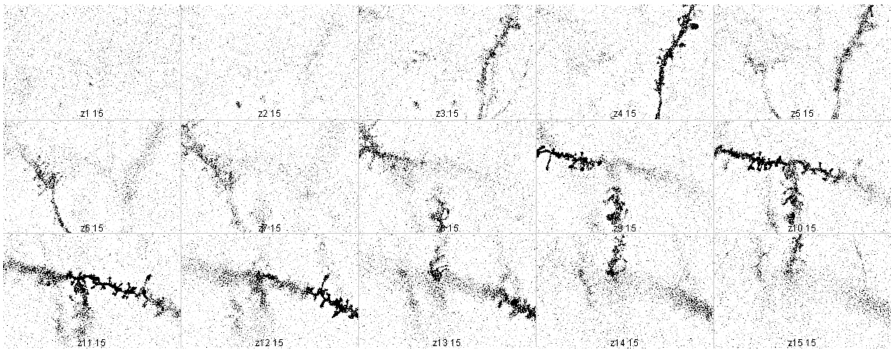


FIGURE 2. A piece of Figure 1. This is a relevant part for our study because we can see there two overlapped dendrites.

Notice that images representing different laboratory techniques must be preprocessed with different algorithms. For this reason, the plugin shows in its dialog window various filters such as median, mean or Gauss filter to reduce noise. Furthermore, to binarize the image we can use *Huang's* threshold algorithm [HW95] or the method of auto thresholding available in ImageJ, called "*Default*", which is a variation of the *IsoData* algorithm [RC78].

Our application is based on the fact that the neuron structure is present or "persists" in many slices or levels of images which belong to a Z-stack. The plugin studies all connected components contained in the different slices, and studies their evolution throughout the Z-stack by means of the zigzag module in (1).

NeuronZigZagJ calculates the main structure and allows one to check automatically whether two dendrites that are linked in the maximal projection of the stack are really the same, or are overlapped on the plane but there is no intersection between them in the space.

The final outputs are two images, see Figure 3. The first one depicts the main connected components of the neuron structure, with different colors. The plugin considers that the main connected components are those that live longer. In this case, there are 4 connected components which live in 11 slices. This Z-stack has 15 slices and these components have the longest life and we can see they represent the main dendritic structure in this image. The second image (right image in Figure 3) is a barcode summary of the life of all connected components which are in the Z-stack.

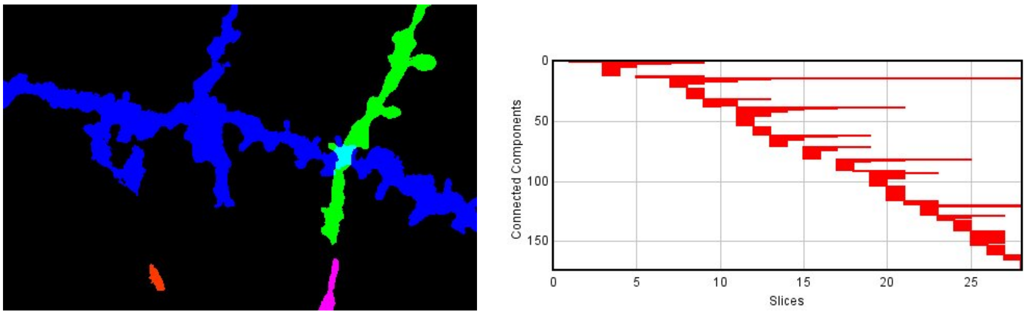


FIGURE 3. Graphical results from the plugin.

REFERENCES

[CdS10] G. Carlsson and V. de Silva. Zigzag persistence. *Foundations of Computational Mathematics*, 10(4):367–405, 2010.

[HMC$^+$13] J. Heras, G. Mata, g. Cuesto, J. Rubio, and M. Morales. Neuron detection in stack images: a persistent homology interpretation. `http://wiki.portal.chalmers.se/cse/pmwiki.php/ForMath/PapersAndSlides`, 2013.

[HW95] L-K Huang and M-J J Wang. Image thresholding by minimizing the measure of fuzziness. *Pattern Recognition*, 28(1):41–51, 1995.

[Mat14] G. Mata. NeuronZigZagJ. University of La Rioja, 2014. `http://spineup.jimdo.com/downloads/`.

[Ras12] W. S. Rasband. ImageJ: Image Processing and Analysis in Java. Technical report, U. S. National Institutes of Health, Bethesda, Maryland, USA, 1997–2012.

[RC78] TW Ridler and S Calvard. Picture thresholding using an iterative selection method. *IEEE Transactions on Systems, Man and Cybernetics*, 8:630–632, 1978.

[RHM$^+$14] A Romero, J. Heras, G. Mata, M. Morales, and J. Rubio. Topo-geometrical processing of neuronal images (in Spanish). *La Gaceta de la RSME*, 17(1):109–128, 2014.

[S$^+$12] J. Schindelin et al. Fiji: an open-source platform for biological-image analysis. *Nature Methods*, 9(7):676–682, 2012.

[ZC05] A. Zomorodian and G. Carlsson. Computing persistent homology. *Discrete and Computational Geometry*, 33(2):249–274, 2005.

Departamento de Matemáticas y Computación. Universidad de La Rioja. Edificio Vives. Calle Luis de Ulloa s/n. 26004 Logroño (La Rioja, Spain).

E-mail address: `{gadea.mata, ana.romero, julio.rubio}@unirioja.es`

SpineUp

E-mail address: `miguelmorales@spineup.es`

UNWINDING PATHS ON THE RIEMANN SPHERE FOR CONTINUOUS INTEGRALS OF RATIONAL FUNCTIONS

ROBERT H. C. MOIR, ROBERT M. CORLESS, AND DAVID J. JEFFREY

1. INTRODUCTION

It is widely understood that computer algebra systems (CAS) and the Risch algorithm and its variants deal with indefinite integrals or antiderivatives. For reasons that will become clear we instead regard the definite integral as fundamental. Consider the following function

$$F(x) = \int_a^x f(t)dt,$$

which is a definite integral once the variable upper limit has been chosen. $F(x)$ unambiguously *is* an antiderivative of $f(x)$. Finding such an $F(x)$ solves the indefinite integration problem.

Doing it this way also solves the problem of continuity in parameters in the integrand as a result of the following

Theorem 1.1. *If $f(x, \xi)$ is separately continuous in x and ξ on a compact interval of $\mathbb{R}^2$, then*

$$F(x, \xi) = \int_a^x f(t, \xi)dt$$

is continuous in x for each ξ and continuous in ξ for each x.

Proof. Provided in almost any book on real analysis. □

Considering the definite integral as fundamental facilitates harmonization of the analytic notion of continuity with the algebraic methodology of the Risch algorithm. For integrals of continuous functions $f(x; \xi)$ that continue to lie within some elementary extension of a function field containing f as ξ is varied, the expression for the integral ought to be continuous. And the integral certainly ought to be continuous in x for fixed ξ. But this is not the case in practice for many CAS even for many simple integrals. For example, when asked to integrate $1/(2 + \sin t)$, MAPLE returns

$$\int \frac{dt}{2 + \sin t} = \frac{2}{\sqrt{3}} \arctan\left(\frac{2\tan(\frac{t}{2}) + 1}{\sqrt{3}}\right), \tag{1}$$

which is discontinuous whenever $t = (2n + 1)\pi$ because the tangent function in the argument of the arctangent function becomes infinite there. Since the arctangent is defined in CAS as the principal branch of $\arctan z$, instead of increasing without bound as $t \to \infty$, the value of the integral (1) cycles endlessly through values in the bounded interval $\left(-\frac{\pi}{\sqrt{3}}, \frac{\pi}{\sqrt{3}}\right)$.

In this paper we consider a way of handling this problem for integrands that are rational functions (*i.e.*, in $\mathbb{R}(x)$) in terms of an extension of the concept of an unwinding number introduced by Corless and Jeffrey [1].

2. LIOUVILLE'S THEOREM AND IMPLICIT PATHS OF INTEGRATION THROUGH INFINITY

That these problems are fairly generic for the integration problem follows from (the strong version of) Liouville's theorem, which states that if $f \in F$, where F is a differential field of characteristic 0 with constant field K, then if $\int f = g$ can be expressed in finite terms such that g is in an elementary extension G of F, then the integral can be expressed in the form

$$\int f = \varphi_0 + \sum_{i=1}^{n} c_i \log(\varphi_i),$$

where $\varphi_0, \varphi_i \in F$ and $c_i \in K$ for all $i = 1, \dots, n$. Thus, if any of the functions φ_i have a complex value $\varphi = u + iv$, the expression for the integral of f contains a term of the form

$$\log(\varphi) = \log(u + iv) = \log\left(\sqrt{u^2 + v^2}\right) + i \cdot \text{arctangent}\left(\frac{v}{u}\right).$$

Note that since $\frac{v}{u}$ appears in the argument of the arctangent function, if u has a root or v has a pole in the path of integration, then the integral of f will have a spurious discontinuity similar to the case observed above. Because $\frac{-v}{u} = \frac{v}{-u}$ there is also a spurious discontinuity at $\pm\frac{\pi}{2}$. And, of course, if φ crosses the branch cut for the logarithm along the path of integration, then an additional spurious discontinuity arises from the choice of logarithm function. Thus, spurious discontinuities arising from both choosing a branch of the logarithm and singular arguments of the arctangent function are a quite generic feature of integrals in finite terms—concerns with complex variables and arctangents come together as a result of Liouville's theorem. The discontinuities at $\pm\frac{\pi}{2}$ are not intrinsic to the problem and can be removed as we will see.

The winding number solution that Corless and Jeffrey [1] propose provides a solution to the problem of paths of integration that implicitly cross branch cuts of complex functions, but it does not address the continuity issue arising in cases like that from a diverging argument to an arctangent function. This latter kind of discontinuity is considered by Jeffrey [3], leading to a solution in terms of introducing Heaviside, or step, functions at the locations of discontinuity. The solution we propose here is similar in certain respects to Jeffrey's solution but is simpler and deals with both sources of discontinuity by tracking a second kind of unwinding.

This second kind of unwinding accounts for singular arguments of inverses of functions with poles. This requires thinking of the variation of values of functions along paths of integration not in the Argand plane but on the Riemann sphere. Along the path of integration, the values of arguments of functions in the expression of the integral can pass through the point at infinity of the Riemann sphere and safely emerge from it without leading to discontinuity. This is precisely what happens in the example above when the argument of the arctangent becomes singular, and we can restore continuity to the expression by "unwinding" trips around the Riemann sphere through ∞.

The tangent function and its inverse form a natural example. First note that the image of the real line on the Riemann sphere is a great circle if we include the point at infinity (see figure 1). We will call $\mathbb{R} \cup \{\infty\}$ on the Riemann sphere the *real circle*. Consider the continuous behaviour of r on the real circle. If we increase r from 0 to π, then $\tan r$ completes a full loop around the real circle, passing through ∞ at $r = \frac{\pi}{2}$. Turning things around, then, if we allow r to complete a full loop counterclockwise around the real circle starting from 0 (0 to $+\infty$ and back to 0 from $-\infty$ on the real line), then $\arctan r$ increases from 0 to π, taking the value $\frac{\pi}{2}$ at $r = \infty$. In this way, by keeping track of windings around the real circle passing through the point at infinity, we can define

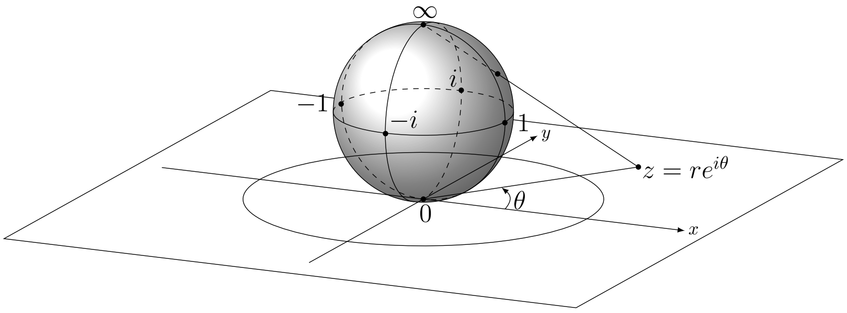


FIGURE 1. The Riemann sphere with the equator as image of the unit circle (shown).

the tangent function over the entire real line and the arctangent function such that $\arctan(\tan r) = r$ for all r on the entire real line.

Now, to consistently analyze unwinding on the Riemann sphere, we cannot cannot use the one-argument definition of the arctangent function because it only covers half of the Riemann sphere, which is the reason for the spurious discontinuities at $\pm\frac{\pi}{2}$. The solution is to use the two-argument definition $\arctan(v, u) = \theta$, where $-\pi < \theta \leq \pi$. Interestingly, this automatically solves the problem for poles of rational functions, because $\arctan(v, u)$ is continuous when $u = 0$. There is still a discontinuity at $\theta = \pm\pi$ when u is negative and v changes sign. But this is handled by the usual unwinding number for the branch cut of the logarithm, which we will call the *angular unwinding number* $\mathcal{K}_\theta(v, u)$. This does not take care of diverging u or v, however, which must be handled with a second unwinding number.

We handle diverging u or v by introducing an additional *radial unwinding number* $\mathcal{K}_r(v, u)$ for the arctangent function, such that for $w(x) = u(x) + iv(x) = re^{i\theta}$, $x \in \mathbb{R}$,

$$\text{invtan}\,(v, u; a) := \text{arctan}\,(v, u) - \text{arctan}\,(v(a), u(a)) + 2\pi\mathcal{K}_\theta\,(v, u; a) + \pi\mathcal{K}_r(v, u; a),$$

where $\mathcal{K}_r(y, x)$ is a count of the number of passes through the point at infinity that *decrease* θ, *i.e.*, where, asymptotically, $v > 0$ and $u > 0$, or $v \geq 0$ and $u < 0$, as $r \to \infty$. Suppressing the constant term, the continuous integral discussed above is then written, correctly, as

$$\int_a^x \frac{dt}{2+\sin t} = \frac{2}{\sqrt{3}}\text{invtan}\Big(2\tan(\tfrac{t}{2}) + 1, \sqrt{3}\Big) = \frac{2}{\sqrt{3}}\Big(\text{arctan}\Big(2\tan(\tfrac{t}{2}) + 1, \sqrt{3}\Big) + \pi\mathcal{K}_r\big(\tan\left(\tfrac{t}{2}\right), 1\big)\Big),$$

since $\mathcal{K}_\theta = 0$. This expression is correct since it is the asymptotic sign of $\tan\left(\frac{t}{2}\right)$ when it becomes singular that determines $\mathcal{K}_r$.

3. CONTINUOUS EXPRESSIONS FOR CONTINUOUS INTEGRALS OF RATIONAL FUNCTIONS

With the arctangent function rendered continuous by adding both an angular and a radial unwinding number, we have the following

Theorem 3.1. *Let f be an element of $\mathbb{K}(t)$ with $\mathbb{K}$ a real closed field. Then if $\int_a^x f(t)dt = g(x)$ for some g in an elementary extension of $\mathbb{K}(x)$, then we can algorithmically find unwinding numbers such that $g(x)$ is a continuous function of x where $f(x)$ is.*

Proof. Too long to include here. The basic idea is that for real rational function integrands, the arctangent terms appearing in the integral are of the form $atan(v, u)$, where $u, v \in \mathbb{K}[x]$, so that

$\mathcal{K}_r(v, u) = 0$ since u and v remain finite. The problem then reduces to computing the angular unwinding number, which requires finding the roots of polynomials in arguments of arctangent functions to determine the sign and the poles of the argument. This can be accomplished algorithmically, for example by using Sturm-Habicht sequences [2]. □

Let us illustrate the theorem with an example. Consider the definite integral

$$\int_{\sqrt{2}}^{x} \frac{t^4 - 3t^2 + 6}{t^6 - 5t^4 + 5t^2 + 4} dx = \arctan\left(\frac{2 - x^2}{x^3 - 3x}\right),$$

a simplified version of what the Risch algorithm yields after reducing a sum of two complex logarithms to two real arctangents and combining them into one. This expression has spurious discontinuities at the roots of $x^3 - 3x$, which we may remove with the two argument arctangent, thereby making the radial unwinding number zero. $\mathcal{K}_\theta$ for the two-argument arctangent is determined by the roots of $2 - x^2$, which indicate locations of sign changes that can cross the branch cut, and the roots of $x^3 - 3x$, which determine if $x^3 - 3x$ is negative when $2 - x^2$ changes sign. With the locations of these roots, it is not difficult to show that

$$\int_{\sqrt{2}}^{x} \frac{t^4 - 3t^2 + 6}{t^6 - 5t^4 + 5t^2 + 4} dx = \arctan\left(2 - x^2, x^3 - 3x\right) + 2\pi\mathcal{K}_\theta\left(2 - x^2, x^3 - 3x\right),$$

where $\mathcal{K}_\theta$ is 0 on $(-\infty, \sqrt{2}]$ as is required since the lower integration limit $\sqrt{2} \in (0, \sqrt{2}]$, and $\mathcal{K}_\theta$ is 1 on $(\sqrt{2}, \infty)$ since $x^3 - 3x$ is negative at $x = \sqrt{2}$ and $2 - x^2$ changes from positive to negative there. Therefore, we may see that for more general rational functions, by using the Sturm-Habicht sequence method of [2] for real root-finding, we can efficiently compute the radial unwinding number to obtain a continuous integral where it exists.

REFERENCES

[1] R. M. CORLESS AND D. J. JEFFREY, *The unwinding number*, ACM SIGSAM Bulletin, 30 (1996), pp. 28–35.

[2] L. GONZÁLEZ-VEGA, T. RECIO, H. LOMBARDI, AND M.-F. ROY, *Sturm-Habicht Sequences, Determinants and Real Roots of Univariate Polynomials*, Springer, 1998.

[3] D. J. JEFFREY, *Integration to obtain expressions valid on domains of maximum extent*, in Proceedings of the 1993 international symposium on Symbolic and algebraic computation, ACM, 1993, pp. 34–41.

Western University, Department of Applied Mathematics, Middlesex College, 1151 Richmond St. N., London (ON), Canada N6A 5B7

E-mail address: rmoir2@uwo.ca, rcorless@uwo.ca, djeffrey@uwo.ca

REPRESENTATION OF FUNCTIONS FOR AN EFFICIENT CAS

DOUGLAS NAVARRO GUEVARA

ABSTRACT. This paper presents a novel and efficient scheme of representation for the common transcendental functions. Such representation is based on a few types of power series characterized by a periodic sequence of numbers that allow the implementation of a coordinate representation of diverse analytical operators. With this approach, the aim is the developement of the core of a CAS under an *object oriented* implementation.

INTRODUCTION

This article shows how the "common transcendental functions"[1] can be written in terms of a few types of power series, characterized by a periodic sequence of numbers. The induced discrete representation allows the definition of a natural isomorphism between some subsets of functions and the space R^n. This isomorphism allows the implementation of a coordinate representation of integration and differentiation operators (among others) very close to the elementary computable functions. Canonical bases in the function spaces can be automatically expressed in terms of standard functions, allowing the development of Computer Algebra Systems (CAS) with orders of execution similar to those of arithmetic calculations.

1. TYPES OF FUNCTIONS, REPRESENTATION AND TREATMENT

For the data structure of the computer application, the $elementary$ complex variable functions are represented by a *"classic binary tree"* structure [2], namely: operands (polynomials or transcendental functions) in the leaves and operators in the interior nodes. When representation of a composition of functions is required the "leaves" point to a new tree.

1.1. **The Types of Functions.** The types of functions considered (namely: $Exponential$, $Geometric$, Arc, $Bessel$ and $Bernoulli$) consist of the functions whose power series expansion at the origin are of the form[2]:

$$(1)\quad \sum_{i=0}^{\infty} b_i\frac{x^i}{i!},\ \sum_{i=max\{0,-k\}}^{\infty} b_i(i+k)!\frac{x^i}{i!},\ \sum_{i=0}^{\infty} b_i(\lfloor i+k\rfloor!)^2\frac{x^i}{i!},\ \sum_{i=0}^{\infty} b_i\frac{1}{(i+k)!i!}x^i,\ \sum_{i=0}^{\infty} b_i\frac{\mathbf{B}_{i+k}}{i!}x^i$$

where (b_i) is a periodic sequence of period n, $k \in Z$, $\mathbf{B}_n$ is the nth Bernoulli number and

$$(2)\qquad \lfloor m\rfloor! = \{1 \text{ if } m \leqslant 0;\ \ 1\,.\,3\,.\,5\,. ...m \text{ if } m \text{ is odd};\ \ 1\,.\,3\,.\,5\,. ...(m-1) \text{ if } m \text{ is even}.$$

Coding. Coding of a function of the *X Type* is made by $F[X; k; b_0, b_1, \cdots, b_{n-1}](x)$, where n is the period of this generatrix sequence.

[1] *E.g.*: exp(x), sin(x), cos(x), sinh(x), cosh(x), arctan(x), arctanh(x), ln(1-x), arcsin(x), arcsinh(x), 1/(1-x), etc. In fact, a subset of functions that intersects the set of holonomic functions [9].

[2] In all cases the radius of convergence can be easily calculated.

Decoding. Decoding is based upon the fact that, for a given length n, a given k and a fixed type, the defined set of functions forms an n-dimensional vector space. As an example, for the $Exponential$ $Type$, the isomorphism is given by the function $\varphi : R^n \longrightarrow B_n$:

$$\varphi(b_0, b_1, ..., b_{n-1}) = \sum_{i=0}^{\infty} b_i \frac{x^i}{i!} \quad where \quad B_n = \left\{ \sum_{i=0}^{\infty} b_i \frac{x^i}{i!} \text{ with } b_i = b_{i+n} \right\}. \tag{3}$$

Fundamental Properties. The sum and scalar multiplication in B_n correspond to the usual vector operations in R^n. The differentiation operator (integration with constant b_n) corresponds to a circular left (right) shift of the generatrix sequence and the unitary increase (decrease) of k (if any). Other properties of R^n are also transferred by the isomorphism φ.

1.2. **Examples.**

Example 0. Coding the function $e^x + \sin(x)$:
It is an $Exponential$ type and corresponds to $(Exp; 1)$ + $(Exp; 0, 1, 0, -1)$=$(Exp; 1, 1, 1, 1)$ + $(Exp; 0, 1, 0, -1)$=$(Exp; 1, 2, 1, 0)$.
Example 1. Decoding the series $F[Geo; -1; 1, 2, 3, 4]$:

$$2\frac{x}{1} + 3\frac{x^2}{2} + 4\frac{x^3}{3} + \frac{x^4}{4} + 2\frac{x^5}{5} + 3\frac{x^6}{6} + 4\frac{x^7}{7} + \frac{x^8}{8} + ... \tag{4}$$

Solution. In the $Geometric\ Type$ the functions corresponding to the base: {[-1; 1,0,1,0], [-1; 0,1,0,1], [-1; 1,0,-1,0], [-1; 0,1,0,-1]} are: {-ln $\left(\sqrt{1-x^2}\right)$, arctanh(x), -ln $\left(\sqrt{1+x^2}\right)$, $\arctan(x)$}. Thus, the sum in question corresponds to:

$$\begin{aligned}[-1; 1, 2, 3, 4] &= 2[-1; 1, 0, 1, 0] + 3[-1; 0, 1, 0, 1] - [-1; 1, 0, -1, 0] - [-1; 0, 1, 0 - 1] \\ &= -2\ln\left(\sqrt{1-x^2}\right) + 3arctanh(x) + \ln\left(\sqrt{1+x^2}\right) - \arctan(x)\end{aligned} \tag{5}$$

Example 2. Consider the automatic reduction of the identity[3]: $\sinh^2(x)$+$\cosh^2(x)$-$\cosh(2x)$.
$Solution.$ The simplification is immediate from the treatment of products and sums[4]:

$$\begin{aligned}&[Exp; 0, 1]^2(x) + [Exp; 1, 0]^2(x) - [Exp; 1, 0](2x) \\ &= -1/2 + [Exp; 1, 0,](2x)/2 + 1/2 + [Exp; 1, 0](2x)/2 - [Exp; 1, 0](2x) \\ &= [Exp; 1, 0](2x) - [Exp; 1, 0](2x) = 0 * [Exp; 1, 0](2x) = 0\end{aligned} \tag{6}$$

Example 3. Consider the solution of the differential equation: y''+y'=e^x+$\sin(x)$.
Coding. If $y(x)$ corresponds to a vector of the form (a, b, c, d). Then, $y'(x)$ corresponds to (b, c, d, a) and $y''(x)$ corresponds to (c, d, a, b), so the equation in question would be written (c, d, a, b)+ $(b, c, d, a) = (1, 2, 1, 0)$ (e^x+$\sin(x)$ as in the *Example 0*) *i.e.*

$$\begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix} = \begin{bmatrix} 1 \\ 2 \\ 1 \\ 0 \end{bmatrix} \tag{7}$$

[3] It is worth noting that the problem of solving equivalences is, in general, recursively undecidable [6].

[4] All products of the elements of the basis A={$\cosh(x)$, $\sinh(x)$, $\cos(x)$, $\sin(x)$} of B_4 (*i.e.* {[1,0,1,0], [0,1,0,1], [1,0,-1,0], [0,1,0,-1]}) are explicitly calculable.

Solution[5]. The solution is then: (1,-1,2,0)+d(-1,1,-1,1).

Decoding. The solution corresponds (with a change of base to the base A of B_4) to:

$$(8)\quad 3\cosh(x)/2 \;-\; \sinh(x)/2 \;-\; \cos(x)/2 \;-\; \sin(x)/2 \;+\; d(\sinh(x) \;-\; \cosh(x))$$

Example 4. It is natural to consider the function $T : F[Geo] \to F[Arc]$ such that:T(F[Geo; k;b])= F[Arc;k;b]. This transformation preserves the solutions of the support space of ordinary differential equations with constant coefficients, that is:

$$a_n y^{(n)} + a_{n-1} y^{(n-1)} + ... + a_1 y' + a_0 y = F[Geo; k; b] \tag{9}$$

solved on $F[Geo]$ is equivalent (*i.e.* the coordinates of the solutions are the same) to:

$$a_n y^{(n)} + a_{n-1} y^{(n-1)} + ... + a_1 y' + a_0 y = F[Arc; k; b] \tag{10}$$

solved on $F[Arc]$. It is the same if the coefficients are polynomials of variable x.

2. Comparison with Mathematica

Below there are some illustrations of the limitations of a leading commercial CAS (Mathematica) by contrast with this approach.

Example 5. Sum of a series

Consider the sum of the *Example 1.* and the Mathematica command:

```
Sum[x^(4n)/((4n))+2x^(4n+1)/((4n+1))+3x^(4n+2)/((4n+2))
    +4x^(4n+3)/((4n+3)),{n,1,Infinity}]
```

Resulting in:

```
1/12 (-24x-18x^2-16x^3+18ArcTanh[x^2]+24x
Hypergeometric2F1[1/4,1,5/4,x^4]+16x^3
Hypergeometric2F1[3/4,1,7/4,x^4]-3Log[1-x^4])
```

Example 6. Identities reduction

Consider the identity of the *Example 2.* and the Mathematica commands:

```
f(x_)=Sinh(x)Sinh(x)+Cosh(x)Cosh(x)-Cosh(2x)
g(x_)=f(x)^2
```

Producing respectively:

```
:Cosh[x]^2-Cosh[2x]+Sinh[x]^2
:(Cosh[x]^2 - Cosh[2x] + Sinh[x]^2)^2
```

Example 7. Solution of differential equations: y''+y'=$(1 + x - x^2)/(1 - x^2)^{\frac{3}{2}}$.

With Mathematica

```
DSolve[y''[x]+y'[x]==(1+x-x^2)/(Sqrt[(1-x^2)^3]),y[x],x]
```

$$(11)\quad y(x) \to \int_1^x \left(c_1 e^{-K[2]} + e^{-K[2]} \int_1^{K[2]} \frac{e^{K[1]}\left(-K[1]^2 + K[1] + 1\right)}{\sqrt{-\left(K[1]^2 - 1\right)^3}} \, dK[1] \right) dK[2] + c_2$$

With the approach proposed here

The function $(1{+}x{-}x^2)/(1{-}x^2)^{\frac{3}{2}}$ is:$F[Arc; 0; 1](x)$. The function y must be of the form:$F[Arc; -2; a](x)$

[5] In an exhaustive process, the solution on the class of polynomial type functions must be considered.

but because this function does not have a proper name it will be considered as $F[Arc;-2;a,b](x)$ then $y' = F[Arc;-1;b,a](x)$ which in this type is equal to $F[Arc;0;b,a](x)$ and $y'' = F[Arc;0;a,b](x)$. Then $y'' + y' = F[Arc;0;1,1](x) = F[Arc;0;a+b,a+b](x)$ requires that a+b=1 and $y = F[Arc;-2;0,1](x) = \arcsin(x)$ is then a solution.

3. Remarks

The representation of algebraic expressions by binary trees and the definition of fundamental analytical calculations allow the definition of the basic $classes$ and $methods$ to develop an efficient CAS from the *object oriented programming paradigm* which calculates directly on the representations. This is very important for a project that have his natural development under this paradigm and needs to be able to handle symbolic computations (as in [5]).

This approach consists of three stages (encoding - computing - decoding). Stage 1 has a minimal cost; stage 2 is the strongest factor for the computational process; and finally the stage 3, which is executed only for the terminal value.

The limitations of a standard CAS versus one developed with the approach proposed here in certain cases are dramatic, not only in terms of execution time, but also in terms of the numerical error produced when attempting to use the analytical results in numerical calculations. *E.g.* you can consider the solution of y''=ln$(1-x)$ by Mathematica (DSolve[y"[x]==Ln[1-x],y[x],x]) versus the non polynomial solution by this approach:

$$y(x) \to \int_1^x \left(\int_1^{K[2]} \mathrm{Ln}(1-K[1])\, dK[1] \right) dK[2] + c_2 x + c_1 \tag{12}$$

$$\int^{(2)} [Geo;-1;-1](x) = [Geo;-3;-1](x) = (1-x)^2(\ln(1-x) - 3/2)/2 \tag{13}$$

References

[1] Abramowitz, M., Stegun, I.: Handbook of Mathematical Functions. Dover Publications, New York (1964)

[2] Cormen, T., Leiserson, Ch., Rivest, R.: Introduction to algorithms. The MIT Press, Cambridge, Massachusetts (1990)

[3] Davenport, J., Siret, Y., Tournier, E.: Calcul formel: systèmes et algorithmes de manipulations algébriques. Masson, Paris (1987)

[4] Hennie, F.: Introduction to Computability. Massachusetts Institute of Technology, University of California, Addison-Wesley, Massachusetts (1977)

[5] Navarro, D., Navarro, A.: Computer Aided Geometry. International Congress on Mathematical Software, Seoul (2014)

[6] Richardson, D.: Some undecidable Problems Involving Elementary Functions of a Real Variable. The Journal of Symbolic Logic, 33, 514–520 (1968)

[7] Risch, R.: The problem of integration in finite terms. Transactions of American Mathematical Society, 139, 167–189 (1969)

[8] Wolfram, S.: Mathematica Book. Cambridge University Press, USA (1999)

[9] Zeilberger, D.: A holonomic systems approach to special functions identities. Journal of Computational and Applied Mathematics, 32, 321–368 (1990)

Universidad Nacional, Heredia, Costa Rica
E-mail address: navarro.douglas@gmail.com

ULTRAQUADRICS ASSOCIATED TO AFFINE AND PROJECTIVE AUTOMORPHISMS

TOMÁS RECIO, J. RAFAEL SENDRA, LUIS F. TABERA, AND CARLOS VILLARINO

ABSTRACT. In this extended abstract, we study the properties of ultraquadrics associated with automorphisms of the field $\mathbb{K}(\alpha)(t_1, \ldots, t_n)$, defined by linear rational (with common denominator) or by polynomial (with polynomial inverse) coordinates. We conclude that ultraquadrics related to polynomial automorphisms can be characterized as varieties $\mathbb{K}-$isomorphic to linear varieties, while ultraquadrics arising from projective automorphisms are isomorphic to the Segre embedding of a blowup of the projective space along an ideal and, in some general case, linearly isomorphic to a toric variety. This information helps us to compute a parametrization of some ultraquadrics.

1. INTRODUCTION

The study and analysis of ultraquadrics was introduced in [2] as a higher dimensional generalization of the concept of hypercircle (cf. [1], [4], [5], [6]) and as a fundamental computational tool to algorithmically solve the problem of the optimal algebraic reparametrization of rational varieties of arbitrary dimension (e.g. rational surfaces, see [3]).

Given a rational variety $\mathcal{V}$, presented by a rational parametrization with n parameters $t_1, \ldots, t_n$ and coefficients in a certain algebraic extension $\mathbb{K}(\alpha)$ of a ground field $\mathbb{K}$, it is natural to ask for the possibility of reparametrizing $\mathcal{V}$ over $\mathbb{K}$. For this purpose the paper [2] introduces the concept of "ultraquadrics" as varieties associated to automorphisms of the field $\mathbb{K}(\alpha)(t_1, \ldots, t_n)$, and describes its application to computing the reparametrization of $\mathcal{V}$ over $\mathbb{K}$, when possible.

In this extended abstract, we study the ultraquadrics associated to some important kind of automorphisms in the field $\mathbb{K}(\alpha)(t_1, \ldots, t_n)$, such as those defined by linear rational (with common denominator) or polynomial (with inverse also polynomial) coordinates. The provided results reinforce the computational usefulness of ultraquadrics.

A complete version of this extended abstract has been submitted to a journal.

1.1. **Notation.** In the sequel, $\mathbb{K}$ is a field of characteristic zero, α is an algebraic element over $\mathbb{K}$, $\mathbb{L}$ is the field extension $\mathbb{K}(\alpha)$ and $\mathbb{F}$ is the algebraic closure of $\mathbb{L}$. So $\mathbb{K} \subset \mathbb{L} = \mathbb{K}(\alpha) \subset \mathbb{F}$. We assume that $[\mathbb{K} : \mathbb{L}] = r$. We use the notation $\overline{t} = (t_1, \ldots, t_n)$ and $\overline{T} = (t_0 : \ldots : t_n)$ for affine –respectively, projective– coordinates.

On the other hand, we will consider the following three groups of automorphisms under composition:
• $\mathbf{B}_{\mathbb{L}}$ is the group of all $\mathbb{L}$-birational transformations (i.e. $\mathbb{L}$-definable) of $\mathbb{F}^n$ onto $\mathbb{F}^n$.
• $\mathbf{A}_{\mathbb{L}}$ is the group of all $\mathbb{L}$-automorphism of the affine space $\mathbb{F}^n$; that is, the subgroup of $\mathbf{B}_{\mathbb{L}}$ where the transformation and its inverse are both described through polynomial coordinates.
• $\mathbf{PGL}_{\mathbb{L}}(n)$ is the group of all $\mathbb{L}$-automorphism of the projective space $\mathbb{P}^n(\mathbb{F})$. Elements in

$\mathbf{PGL}_{\mathbb{L}}(n)$ are represented by a $(n+1)\times(n+1)$ regular matrix L

$$\mathbb{P}^n(\mathbb{F}) \to \mathbb{P}^n(\mathbb{F});\ \overline{T} \mapsto L\cdot(\overline{T}^{\,t}) = [L_0(\overline{T}):\dots:L_n(\overline{T})] \tag{1}$$

where the rows L_i of L represent linear forms.

1.2. **Ultraquadrics.** Let $\Psi=(\psi_1,\dots,\psi_n)$ be a birational automorphism of $\mathbb{F}^n$. Then, we express Ψ in the basis $\{1,\dots,\alpha^{r-1}\}$ as

$$\Psi(\bar{t}) = \left(\sum_{j=0}^{r-1}\psi_{1,j}\alpha^j,\dots,\sum_{j=0}^{r-1}\psi_{n,j}\alpha^j\right),\quad \psi_{ij}\in\mathbb{K}(\bar{t}).$$

Then, using this notation, we consider the expansion map

$$\begin{array}{llll} \mathrm{U}: & \mathbf{B}_{\mathbb{L}} & \to & \mathbb{K}(\bar{t})^{nr} \\ & \Psi(\bar{t}) & \mapsto & (\psi_{10}(\bar{t}),\dots,\psi_{1(r-1)}(\bar{t}),\dots,\psi_{n0}(\bar{t}),\dots,\psi_{n(r-1)}(\bar{t})) \end{array} \tag{2}$$

We define the ultraquadric associated with Ψ, and we denote it by $\mathrm{U}ltra(\Psi)$, as the rational variety of dimension n in $\mathbb{F}^{nr}$ parametrized by $\mathrm{U}(\Psi(\bar{t}))$. Different automorphisms Ψ_1, Ψ_2 may define the same ultraquadric $\mathrm{U}ltra(\Psi_1)=\mathrm{U}ltra(\Psi_2)$. This can happen if and only if $\Psi_2=\Psi_1\circ\Phi$ with Φ an automorphism in $\mathbf{B}_{\mathbb{L}}$ with coefficients in $\mathbb{K}$. We define $[\Psi]$ as the coset $[\Psi]=\{\Psi\circ\Phi|\Phi\in\mathbf{B}_{\mathbb{L}}$ with coefficients in $\mathbb{K}\}$.

If $\Psi\in\mathbf{PGL}_{\mathbb{L}}(n)$, say $\Psi(\overline{T})=[L_0(\overline{T}):\dots:L_n(\overline{T})]$, we will denote as $\mathrm{U}ltra(\Psi)$ the (affine) ultraquadric generated by the associated affine mapping

$$\Psi_a(\bar{t}) = \left(\frac{L_1(1,t_1,\dots,t_n)}{L_0(1,t_1,\dots,t_n)},\dots,\frac{L_n(1,t_1,\dots,t_n)}{L_0(1,t_1,\dots,t_n)}\right) \tag{3}$$

2. Ultraquadrics associated to affine and projective automorphisms

Next statement characterizes the ultraquadrics associated with automorphisms in $\mathbf{A}_{\mathbb{L}}$.

Theorem 2.1. *Let $\Psi\in\mathbf{B}_{\mathbb{L}}$. The following statements are equivalent*

(1) $\mathrm{U}ltra(\Psi)$ *is $\mathbb{K}$-isomorphic to $\mathbb{F}^n$.*

(2) $[\Psi]\cap\mathbf{A}_{\mathbb{L}}\neq\emptyset$.

Moreover, $\mathrm{U}ltra(\Psi)$ *is a linear variety if and only if* $[\Psi]$ *contains a linear automorphism.*

Proof. (sketch) A $\mathbb{K}$-definable proper parametrization $\mathcal{P}(\bar{t})=(P_{10},\dots,P_{1(r-1)},\dots,P_{n0},\dots,P_{n(r-1)})$ parametrizes $\mathrm{U}ltra(\Psi)$ if and only if $\mathcal{Q}(\bar{t}):=(\sum_{j=0}^{r-1}P_{1,j}\alpha^j,\dots,\sum_{j=0}^{r-1}P_{n,j}\alpha^j)\in[\Psi]$. Now, $\mathcal{P}^{-1}$ is the expansion map obtained from $\mathcal{Q}^{-1}$. Hence, $\mathcal{P}$ and $\mathcal{P}^{-1}$ are polynomial (resp. linear) if and only if $\mathcal{Q}$ and $\mathcal{Q}^{-1}$ are polynomial (resp. linear). □

Now, we study the case of projective automorphisms. Let $\Psi=L\in\mathbf{PGL}_{\mathbb{L}}(n)$, we describe the structure of $\mathrm{U}ltra(\Psi)$ as a blowup of $\mathbb{P}^n(\mathbb{F})$, (see [7]). Write Ψ as

$$\Psi(\overline{T}) = L\cdot\overline{T}^{\,t} = [L_0(\overline{T}):L_1(\overline{T}):\dots:L_n(\overline{T})]$$

where L_i is the linear form represented by the i-th row of L. Let $\alpha=\alpha_1,\alpha_2,\dots,\alpha_r$ be the conjugates of α in $\mathbb{F}$ and let $\sigma_1,\dots,\sigma_r$ be $\mathbb{K}$-automorphisms of $\mathbb{F}$ such that $\sigma_i(\alpha)=\alpha_i$, and let g_i be the form of degree $r-1$ that is the product of all conjugate forms $\{L_0^{\sigma_1},\dots,L_0^{\sigma_r}\}$ with the exception of $L_0^{\sigma_i}$; where L^{σ_i} is the linear form obtained from L substituting α by α_i. Furthermore, let $I=(g_1,\dots,g_r)$ be the homogeneous ideal generated by $\{g_1,\dots,g_r\}$ in $\mathbb{F}[t_0,\dots,t_n]$. Then

Theorem 2.2. *The projective closure of the ultraquadric* $\mathrm{U}ltra(\Psi)$ *is* $\mathbb{L}$*-linearly isomorphic to the Segre embedding of the blowup of* $\mathbb{P}^n(\mathbb{F})$ *along the ideal* I*.*

Proof. We consider the map

$$\begin{array}{rccc} \eta: & \mathbb{P}^n(\mathbb{F}) & \longrightarrow & \mathbb{P}^n(\mathbb{F}) \times \mathbb{P}^{r-1}(\mathbb{F}) \\ & \overline{T} & \mapsto & (\overline{T}\ ;\ (g_1(\overline{T}) : g_2(\overline{T}) : \ldots : g_r(\overline{T}))) \end{array}$$

which is a blowup of $\mathbb{P}^n(\mathbb{F})$ along I. Now, we compose this map with the Segre embedding of $\mathbb{P}^n(\mathbb{F}) \times \mathbb{P}^{r-1}(\mathbb{F})$ to get the blowup of $\mathbb{P}^n(\mathbb{F})$ as isomorphic to the subvariety $\mathcal{W}$ of $\mathbb{P}^{rn+r-1}(\mathbb{F})$ parametrized by $P := [t_0g_1 : \ldots : t_0g_r : \ldots : t_ng_1 : \ldots : t_ng_r]$. On the other hand, $\mathrm{U}ltra(\Psi)$ is (linearly) $\mathbb{L}$-isomorphic to the affine variety $\mathcal{V}$ parametrized by $\Psi_a \times \Psi_a^{\sigma_2} \times \cdots \times \Psi_a^{\sigma_r}$ (see [3]). Projectively, the parametrization $\Psi_a \times \Psi_a^{\sigma_2} \times \cdots \times \Psi_a^{\sigma_r}$ can be expressed as $[L_0g_1 : L_1g_1 : \ldots : L_ng_1 : L_1^{\sigma_2}g_2 : \ldots : L_n^{\sigma_2}g_2 : \ldots : L_1^{\sigma_r}g_r : \ldots : L_n^{\sigma_r}g_r]$. This variety is isomorphic to the subvariety of $\mathbb{P}^{nr+r-1}$ parametrized by

$$Q := [L_0g_1 : \ldots : L_ng_1 : L_0^{\sigma_2}g_2 : \ldots : L_n^{\sigma_2}g_2 : \ldots : L_0^{\sigma_r}g_r : \ldots : L_n^{\sigma_r}g_r]$$

since $L_0^{\sigma_i}g_i = L_0g_1$, and we are just duplicating the first coordinate of each block.

Since by definition $\Psi^{\sigma_i}(\overline{T})^t = L^{\sigma_i} \cdot \overline{T}^t$, then

$$Q = (g_i\Psi^{\sigma_i})^t = L^{\sigma_i}(g_i \cdot \overline{T})^t$$

where the super-index t denotes the transpose of the matrix. Finally observe that the parametrization provided by the right side of the formula above is just a re-ordering of the coordinates of P. Thus, $\mathcal{W}$ is linearly isomorphic to the projective closure of $\mathrm{U}ltra(\Psi)$. □

Remark 2.3. The center of the blowup, i.e. the variety defined by the ideal I, is

$$\mathcal{Z} = \bigcup_{L^{\sigma_i} \neq L^{\sigma_j}} \{L_0^{\sigma_i} = L_0^{\sigma_j} = 0\}.$$

If L_0 does not have coefficients in $\mathbb{K}$, then the ultraquadric is not a linear variety.

Corollary 2.4.

(1) $\mathrm{U}(\Psi)$ *is an isomorphism of* $\mathbb{P}^n(\mathbb{F}) \setminus \mathcal{Z}$ *onto its image. In particular, the affine part of* $\mathrm{U}ltra(\Psi)$ *is always smooth.*
(2) *Let* $r \leq n$ *and let* $L_0^{\sigma_1}, \ldots, L_0^{\sigma_r}$ *be hyperplanes in general position in* $\mathbb{P}^n(\mathbb{F})$*. Then, the ultraquadric* $\mathrm{U}ltra(\Psi)$ *is (linearly isomorphic to) a toric variety.*

In some applications it is interesting to restrict to real-complex case and surfaces, see for instance [3]. Hence, we take now a closer look to the case of algebraic extensions of degree $r = 2$ and automorphisms of $\mathbb{P}^2(\mathbb{F})$. Next result describes in this context the intersection of ultraquadrics with the hyperplane at infinity (cf. [4] for the hypercircle case).

Corollary 2.5. *Let* $r = 2$*,* $\Phi = [L_0 : L_1 : L_2] \in \mathbf{PGL}_{\mathbb{L}}(2)$*, let* $x^2 + ax + b$ *be the minimal polynomial of* α *over* $\mathbb{K}$*.*

(1) *If the primitive part of* L_0 *is in* $\mathbb{K}[s,t]$*, then* $\mathrm{U}ltra(\Psi)$ *is a plane.*
(2) *If the primitive part of* L_0 *is in* $\mathbb{L}[s,t] \setminus \mathbb{K}[s,t]$*, then* $\mathrm{U}ltra(\Psi)$ *is linearly isomorphic to a blowup of the plane at a point. In particular, it is smooth.*

Moreover, let $\{L_0 = 0\}$ *and* $\{L_0^\sigma = 0\}$ *be the lines defined, respectively, by the denominator and by its conjugate, let* $p = \{L_0 = L_0^\sigma = 0\}$ *be the intersection point. Then, the intersection of* $\mathrm{U}ltra(\Psi)$ *with the hyperplane at infinity consists in three lines* $\mathcal{L}$, $\mathcal{L}^\sigma$, E. *Furthermore:*

(1) $\mathrm{U}ltra(\Psi)$ *is the blowup of the plane at* p.
(2) $\mathcal{L}$ *does not depend on* Ψ *(and hence neither does* $\mathcal{L}^\sigma$*), it only depends on the minimal polynomial of* α. *In fact* $\mathcal{L} = V(\{x_0, 2x_1 - (2\alpha + a)x_2, 2x_3 - (2\alpha + a)x_4\})$.
(3) $q = [0 : (\alpha + a/2)L_1(p) : L_1(p), (\alpha + a/2)L_2(p) : L_2(p)] \in \mathcal{L}$ *is such that* $\mathcal{L} \setminus \{q\}$ *corresponds, by the parametrization, to* $\{L_0 = 0\} \setminus \{p\}$.
(4) $E = \langle q, q^\sigma\rangle$, *the line through* q *and* q^σ, *is the exceptional divisor of the blowup.*

Example 2.6. Consider the extension $\mathbb{R} \subseteq \mathbb{R}(\mathrm{i}) = \mathbb{C}$ and the automorphism of the plane given by $L(t_0 : t_1 : t_2) = (t_1 + \mathrm{i}t_2, t_0, t_1)$. Then $L_0 = \{t_1 + \mathrm{i}t_2 = 0\}$, $L_0^\sigma = \{t_1 - \mathrm{i}t_2 = 0\}$. The center of the blowup is the origin $(1 : 0 : 0)$. $\mathrm{U}ltra(L) = V(x_2x_3 - x_1x_4, x_3 - x_3^2 - x_4^2, x_1 - x_1x_3 - x_2x_4) \subseteq \mathbb{C}^5$. The projectivization of $\mathrm{U}ltra(L)$ intersects the hyperplane at infinity at the three lines $\mathcal{L} = V(x_0, x_1 - \mathrm{i}x_2, x_3 - \mathrm{i}x_4)$, $\mathcal{L}^\sigma = V(x_0, x_1 + \mathrm{i}x_2, x_3 + \mathrm{i}x_4)$ and $E = V(x_0, x_3, x_4)$. In this case $q = (0 : \mathrm{i} : 1 : 0 : 0)$. This information suggests to parametrize the ultraquadric by intersecting it with the pencils of hyperplanes $x_1 + ix_2 = t$, $x_3 + ix_4 = s$, yielding the parametrization $x_1 = st/(2s - 1)$, $x_2 = (s - 1)t/(2is - i)$, $x_3 = s^2/(2s - 1)$, $x_4 = (-is^2 + is)/(2is - 1)$.

ACKNOWLEDGEMENTS

Authors supported by the Spanish *Ministerio de Economía y Competitividad* and by the European Regional Development Fund (ERDF), under the Project MTM2011-25816-C02-(01,02). J. R. Sendra and C. Villarino are members of the research group ASYNACS (Ref. CCEE2011/R34).

REFERENCES

[1] C. Andradas, T. Recio and J. R. Sendra. Base field restriction techniques for parametric curves. *Proc. ISSAC99, ACM Press*, 1:17–22, 1999.
[2] C. Andradas, T. Recio, J. R. Sendra and L. F. Tabera. On the simplification of the coefficients of a parametrization. *J. Symbolic Comput.*, 44(2):192–210, 2009.
[3] C. Andradas, T. Recio, J. R. Sendra, L. F. Tabera and C. Villarino. Proper Real Reparamtrization of Rational Ruled Surfaces. *Computer Aided Geometric Design*, 28(2):102–113, 2011.
[4] T. Recio, J. R. Sendra, L. F. Tabera and C. Villarino. Generalizing circles over algebraic extensions. *Math. Comp.*, 79(270):1067–1089, 2010.
[5] T. Recio, J. R. Sendra, L. F. Tabera and C. Villarino. Algorithmic Detection of Hypercircles. *Mathematics and Computers in Simulation*, 82(1):54–67, 2011.
[6] T. Recio, J. R. Sendra and C. Villarino. From Hypercircles to Units. *Proc. ISSAC-2004 ACM-Press*, 1:258–265, 2004.
[7] K.E. Smith, L. Kahanpää, P. Kekäläinenn, W. Traves. An Invitation to Algebraic Geometry. Universititext, Springer Velag, 2000.

Departamento de Matemáticas, Estadística y Computación, Universidad de Cantabria, 39071, Santander, Spain
E-mail address: `tomas.recio@unican.es, luisfelipe.tabera@unican.es`

Dpto. de Física y Matemáticas, Universidad de Alcalá E-28871, Alcalá de Henares, Madrid, Spain
E-mail address: `rafael.sendra@uah.es, carlos.villarino@uah.es`

FAMILIES OF NUMERICAL SEMIGROUPS: FROBENIUS PSEUDO-VARIETIES AND TREES ASSOCIATED TO THEM

AURELIANO M. ROBLES-PÉREZ AND JOSÉ CARLOS ROSALES

ABSTRACT. In order to collect common properties of several families of numerical semigroups, the concept of Frobenius pseudo-variety is introduced. Moreover, we study the tree structure that arise with it.

1. INTRODUCTION: SOME RESULTS ON NUMERICAL SEMIGROUPS

Let $\mathbb{Z}$ and $\mathbb{N}$ be the sets of integers and non-negative integers, respectively. A *submonoid* of $\mathbb{N}$ is a set $M \subseteq \mathbb{N}$ that contains the zero element and is closed under addition. A *numerical semigroup* is a submonoid S of $\mathbb{N}$ such that $\mathbb{N} \setminus S$ is finite. Notable elements of a numerical semigroup S are $\mathrm{F}(S) = \max(\mathbb{Z} \setminus S)$ (*Frobenius number of* S), $\mathrm{g}(S) = \sharp(\mathbb{N} \setminus S)$ (*genus of* S), and $\mathrm{m}(S) = \min(S \setminus \{0\})$ (*multiplicity of* S). (As usual, $\sharp A$ denotes the cardinality of A.)

Remark 1.1. The content of this section can be seen (or easily deduced from the results that appear) in [4] and the references therein.

Given a non-empty set $A \subseteq \mathbb{N}$, the submonoid of $\mathbb{N}$ generated by A is the set

$$\langle A \rangle = \{\lambda_1 a_1 + \cdots + \lambda_n a_n \mid n \in \mathbb{N} \setminus \{0\},\ a_1, \ldots, a_n \in A,\ \lambda_1, \ldots, \lambda_n \in \mathbb{N}\}.$$

If this is the case, we say that A is a *system of generators* of M. Moreover, if $M \neq \langle B \rangle$ for every $B \subsetneq A$, then A is a *minimal system of generators* of M. It is well known that every submonoid of $\mathbb{N}$ has a unique minimal system of generators, which in addition is finite. On the other hand, $\langle A \rangle$ is a numerical semigroup if and only if $\gcd(A) = 1$.

If X is the minimal system of generators of a numerical semigroup S, then $\mathrm{e}(S) = \sharp X$ is the *embedding dimension of* S. It is easy to see that $\mathrm{e}(S) \leq \mathrm{m}(S)$. In particular, if $\mathrm{e}(S) = \mathrm{m}(S)$, then we say that S has *maximal embedding dimension* (see [5]).

It is well known that, if S, T are numerical semigroups (with $S \neq \mathbb{N}$), then $S \cup \{\mathrm{F}(S)\}$ and $S \cap T$ are numerical semigroups too. Moreover, we have the following result.

Theorem 1.2. *Let S, T be numerical semigroups and let $A = \{a_1, \ldots, a_n\}$ be the minimal system of generators of S. Then $S = T \cup \{\mathrm{F}(T)\}$ if and only if $T = S \setminus \{a_i\}$, where a_i is a minimal generator of S such that $a_i > \mathrm{F}(S)$. Moreover, if this is the case, then $\mathrm{F}(S) < \mathrm{F}(T) = a_i$ and $\mathrm{g}(T) = \mathrm{g}(S) + 1$.*

A *(directed) graph* G is a pair (V, E), where V is a non-empty set and E is a subset of $\{(v, w) \in V \times V \mid v \neq w\}$. The elements of V are called *vertices* of G and the elements of E are called *edges* of G. A *path (of length n)* connecting the vertices x and y of G is a sequence of different edges

Both of the authors are supported by FQM-343 (Junta de Andalucía), MTM2010-15595 (MICINN, Spain), and FEDER funds. The second author is also partially supported by Junta de Andalucía/Feder Grant Number FQM-5849.

of the form $(v_0, v_1), (v_1, v_2), \ldots, (v_{n-1}, v_n)$ such that $v_0 = x$ and $v_n = y$. A graph G is a *tree* if there exist a vertex r (known as the *root* of G) such that, for every other vertex x of G, there exists a unique path connecting x and r. If (x, y) is an edge of the tree, then we say that x is a *child* of y.

Let $\mathcal{S}$ be the set formed by all numerical semigroups. Theorem 1.2 allows us to build the tree associated to $\mathcal{S}$, which we denote by $\mathrm{G}(\mathcal{S})$. In this tree, the vertices are the elements of $\mathcal{S}$ (that is, the numerical semigroups), (T, S) is an edge if $S = T \cup \{\mathrm{F}(T)\}$, and $\mathbb{N}$ is the root. On the other hand, if S is a numerical semigroup, then the unique path connecting S with $\mathbb{N}$ is given by (the *chain of numerical semigroups associated to* S) $\mathrm{C}(S) = \{S_0 \subsetneq S_1 \subsetneq \cdots \subsetneq S_n\}$, where $S_0 = S$, $S_{i+1} = S_i \cup \{\mathrm{F}(S_i)\}$, for all $i < n$, and $S_n = \mathbb{N}$.

The next result (see [4, Prop. 7.1]) follows from Theorem 1.2 and the previous paragraph.

Proposition 1.3. *The graph* $\mathrm{G}(\mathcal{S})$ *is a tree with root equal to* $\mathbb{N}$. *Moreover, the children of* $S \in \mathcal{S}$ *are* $S \setminus \{a_1\}, \ldots, S \setminus \{a_r\}$, *where* $a_1, \ldots, a_r$ *are the minimal generators of* S *that are greater than* $\mathrm{F}(S)$.

2. Frobenius varieties

For certain families of numerical semigroups we can observe a similar behaviour to that described in the previous section. For example (see [4]), we have the family of Arf numerical semigroups, the family of saturated numerical semigroups, the family of numerical semigroups having a Toms decomposition, and the family of numerical semigroups defined by a strongly admissible linear homogeneous pattern. This observation led to introduce, in [3], the concept of *(Frobenius) variety*.

Definition 2.1. A *variety* is a non-empty family $\mathcal{V}$ of numerical semigroups that fulfills the following conditions,

(1) if $S, T \in \mathcal{V}$, then $S \cap T \in \mathcal{V}$;
(2) if $S \in \mathcal{V}$ and $S \neq \mathbb{N}$, then $S \cup \{\mathrm{F}(S)\} \in \mathcal{V}$.

Since the intersection of varieties is another variety, we can define the *variety generated by a family of numerical semigroups* $\mathcal{F}$ (denoted by $\mathrm{F}(\mathcal{F})$) as the intersection of all varieties containing $\mathcal{F}$. Let us observe that $\mathrm{F}(\mathcal{F})$ is the smallest, with respect to the inclusion order, variety containing $\mathcal{F}$.

In [3] was shown that several facts, that hold for the above mentioned families (and, as we have said before, that generalize the situation of Section 1), are also satisfied in any variety. Nevertheless, there exist outstanding families that are not varieties, but that preserve such behaviour. For example, the family of numerical semigroups with maximal embedding dimension and multiplicity m is not a variety (see [5]), but satisfies several properties of such families. In order to study this class of numerical semigroups, recently (see [1]) have been introduced the non-homogeneous patterns and, moreover, have been defined the non-homogeneous Frobenius varieties of multiplicity m (or m-varieties for short).

3. Frobenius pseudo-varieties

In order to study families of numerical semigroups that are not varieties, in [2] (see this reference for a detailed development of this section), we introduced the next concept.

Definition 3.1. A *(Frobenius) pseudo-variety* is a non-empty family $\mathcal{P}$ of numerical semigroups that fulfills the following conditions,

(1) $\mathcal{P}$ has a maximum element $\max(\mathcal{P})$ (with respect to the inclusion order);
(2) if $S, T \in \mathcal{P}$, then $S \cap T \in \mathcal{P}$;
(3) if $S \in \mathcal{P}$ and $S \neq \max(\mathcal{P})$, then $S \cup \{\mathrm{F}(S)\} \in \mathcal{P}$.

Remark 3.2. Observe that, in [1], the maximum element of an m-variety $\mathcal{M}$ is the numerical semigroup $\{0, m, \rightarrow\} = \{0, m\} \cup \{z \in \mathbb{N} \mid z > m\}$ and the multiplicity of all numerical semigroups, that belong to $\mathcal{M}$, is equal to m. We have removed these restrictions.

3.1. **Pseudo-varieties and varieties.** From the definitions, it is clear that every variety is a pseudo-variety. However, there are pseudo-varieties that are not varieties. For example, if S is a numerical semigroup different from $\mathbb{N}$, then $\{S\}$ is a pseudo-variety but not a variety.

It is clear that, if $\mathcal{P}$ is a pseudo-variety, then $\mathcal{P}$ is a variety if and only if $\mathbb{N} \in \mathcal{P}$. Furthermore, if $\mathcal{P}$ is a family of numerical semigroups with maximum Δ, then $\mathcal{P}$ is a pseudo-variety if and only if $\mathcal{P} \cup \mathrm{C}(\Delta)$ is a variety.

On the other hand, if $\mathcal{P}$ is a pseudo-variety and $S \in \mathcal{P}$, then $\max(\mathcal{P}) \in \mathrm{C}(S)$. Moreover, if S_1, S_2, Δ are numerical semigroups such that $\Delta \in \mathrm{C}(S_1) \cap \mathrm{C}(S_2)$, then $\Delta \in \mathrm{C}(S_1 \cap S_2)$.

The previous comments allow us to establish the following result.

Theorem 3.3. *Let $\mathcal{V}$ be a variety and let Δ be a numerical semigroup such that $\Delta \in \mathcal{V}$. Then $\mathcal{D}(\mathcal{V}, \Delta) = \{S \in \mathcal{V} \mid \Delta \in \mathcal{C}(S)\}$ is a pseudo-variety. Moreover, every pseudo-variety can be obtained in this way.*

Remark 3.4. If we take $\max(\mathcal{P}) = \mathbb{N}$ in Subsections 3.3 and 3.4, then we recover analogous results for varieties that were shown in [3].

3.2. **Examples of pseudo-varieties.** Let $m \in \mathbb{N}\backslash\{0\}$. Let $\mathcal{S}(m)$ be the set formed by all numerical semigroups that have multiplicity m. It is clear that the family $\mathcal{S}(m)$ is a pseudo-variety. In the same line, the family of all numerical semigroups with maximal embedding dimension and multiplicity m is another pseudo-variety. We must observe that the family of all numerical semigroups with maximal embedding dimension is not a pseudo-variety.

In general, the intersection of pseudo-varieties is not a pseudo-variety. For example, if S_1, S_2 are different numerical semigroups, then $\mathcal{P}_1 = \{S_1\}$ and $\mathcal{P}_2 = \{S_2\}$ are pseudo-varieties, but not $\mathcal{P}_1 \cap \mathcal{P}_2 = \{\emptyset\}$. In spite of all, we can define the *pseudo-variety generated by a family of numerical semigroups* $\mathcal{F}$ (denoted by $\mathfrak{p}(\mathcal{F})$) as the intersection of all pseudo-varieties containing $\mathcal{F}$. In fact, $\mathfrak{p}(\mathcal{F})$ is the intersection of all pseudo-varieties that contain $\mathcal{F}$ and whose maximum is $\Theta(\mathcal{F})$, where $\Theta(\mathcal{F})$ is the numerical semigroup $\min\big(\bigcap_{S \in \mathcal{F}} \mathrm{C}(S)\big)$.

3.3. $\mathcal{P}$**-monoids.** Let $\mathcal{P}$ be a pseudo-variety. We say that a submonoid M of $\mathbb{N}$ is a $\mathcal{P}$-monoid if it can be expressed as an intersection of elements of $\mathcal{P}$. It is obvious that the intersection of $\mathcal{P}$-monoids is a $\mathcal{P}$-monoid.

If $A \subseteq \max(\mathcal{P})$, we define the *$\mathcal{P}$-monoid generated by A*, denoted by $\mathcal{P}(A)$, as the intersection of all the $\mathcal{P}$-monoids containing A (or, equivalently, the intersection of all elements of $\mathcal{P}$ containing A). We have that $\mathcal{P}(A)$ is the smallest (with respect to the inclusion order) $\mathcal{P}$-monoid containing A.

If $M = \mathcal{P}(A)$, then we say that A is a *$\mathcal{P}$-system of generators* of M. In addition, if $M \neq \mathcal{P}(B)$ for every $B \subsetneq A$, then A is a *minimal $\mathcal{P}$-system of generators* of M.

Theorem 3.5. *Every $\mathcal{P}$-monoid has a unique minimal $\mathcal{P}$-system of generators. Additionally, such a $\mathcal{P}$-system is finite.*

3.4. **The tree associated to a pseudo-variety.** For a pseudo-variety $\mathcal{P}$, we define the graph $\mathrm{G}(\mathcal{P})$ in the following way,

- the set of vertices of $\mathrm{G}(\mathcal{P})$ is $\mathcal{P}$;
- $(S, S') \in \mathcal{P} \times \mathcal{P}$ is an edge of $\mathrm{G}(\mathcal{P})$ if and only if $S' = S \cup \{\mathrm{F}(S)\}$.

If $S \in \mathcal{P}$, then we can define recursively the sequence,

- $S_0 = S$,
- if $S_i \neq \max(\mathcal{P})$, then $S_{i+1} = S_i \cup \{\mathrm{F}(S_i)\}$.

We have that $\mathrm{C}_{\mathcal{P}}(S) = \{S_0 \subsetneq S_1 \subsetneq \cdots \subsetneq S_n\}$ (where $S_n = \max(\mathcal{P})$) is precisely the unique path connecting S with $\max(\mathcal{P})$.

Observe that we can construct recursively $\mathrm{G}(\mathcal{P})$ from $\max(\mathcal{P})$. Indeed, it is sufficient to know how to compute the children of each vertex S. Let T a child of S in $\mathrm{G}(\mathcal{P})$, that is, $S = T \cup \{\mathrm{F}(T)\}$ or, equivalently, $T = S \setminus \{\mathrm{F}(T)\}$. Thereby, there exists an integer $x > \mathrm{F}(S)$ such that $T = S \setminus \{x\}$. On the other hand, if M is a $\mathcal{P}$-monoid and $x \in M$, then $M \setminus \{x\}$ is a $\mathcal{P}$-monoid if and only if x belongs to the minimal $\mathcal{P}$-system of generators of M. Thus, we can show the next result (that it is analogue to Proposition 1.3).

Theorem 3.6. *The graph* $\mathrm{G}(\mathcal{P})$ *is a tree with root equal to* $\max(\mathcal{P})$. *Moreover, the children of a vertex* $S \in \mathcal{P}$ *are* $S \setminus \{x_1\}, \ldots, S \setminus \{x_r\}$*, where* $x_1, \ldots, x_r$ *are the elements of the minimal* $\mathcal{P}$*-system of generators of* S *that are greater than* $\mathrm{F}(S)$.

Remark 3.7. Theorem 3.6 can be used to describe and enumerate the members of families of numerical semigroups having certain properties (that lead to the pseudo-variety structure). For example, we have that, if S' is a child of S in $\mathrm{G}(\mathcal{P})$, then $\mathrm{F}(S') > \mathrm{F}(S)$ and $\mathrm{g}(S') = \mathrm{g}(S) + 1$. Therefore, we get numerical semigroups with greater Frobenius number and genus when we go on along the branches of the tree. Thus, we can use this construction in order to obtain all the numerical semigroups, in the pseudo-variety $\mathcal{P}$, with a given Frobenius number or genus.

References

[1] M. Bras-Amorós, P. A. García-Sánchez, A. Vico-Oton, *Nonhomogeneous patterns on numerical semigroups*, Int. J. Algebra Comput. **23** (2013), 1469–1483.

[2] A. M. Robles-Pérez and J. C. Rosales, *Frobenius pseudo-varieties in numerical semigroups*, to appear in Ann. Mat. Pura Appl. doi:10.1007/s10231-013-0375-1.

[3] J. C. Rosales, *Families of numerical semigroups closed under finite intersections and for the Frobenius number*, Houston J. Math. **34** (2008), 339–348.

[4] J. C. Rosales and P. A. García-Sánchez, *Numerical semigroups*, Developments in Mathematics, vol. **20**, Springer, New York, 2009.

[5] J. C. Rosales, P. A. García-Sánchez, J. I. García-García and M. B. Branco, *Numerical semigroups with maximal embedding dimension*, Int. J. Commutative Rings **2** (2003), 47–53.

A.M. Robles-Pérez, Department of Applied Mathematics, University of Granada
E-mail address: `arobles@ugr.es`

J.C. Rosales, Department of Algebra, University of Granada
E-mail address: `jrosales@ugr.es`

POMMARET-SEILER RESOLUTION IS CELLULAR

EDUARDO SÁENZ-DE-CABEZÓN

ABSTRACT. We show that the Pommaret-Seiler resolution for quasi-stable ideals has a cellular structure that generalizes that of the Eliahou-Kervaire resolution for stable ideals. This structure suggests an algorithms for the construction and minimization of the resolution.

A Pommaret basis of a polynomial submodule $\mathcal{M}$ is one kind of involutive basis that has certain features which help the description of the structure of $\mathcal{M}$. Any polynomial submodule has, after an appropriate change of coordinates when necessary, such a basis. If $\mathcal{M}$ is a monomial ideal I then a change of coordinates may change its monomiality, so there are certain monomial ideals that have a finite Pommaret basis, we call these ideals *quasi-stable*. Quasi-stable ideals can be characterised in several ways [14] having different names, such as *ideals of nested type* [2], *ideals of Borel type* [9] or *weakly stable ideals* [4]. They can be seen as a generalization of stable ideals. Stable and quasi-stable ideals appear in different contexts, both computational and theoretical, in particular in relation to generic initial ideals. In [14] Seiler constructs a (nonminimal) free resolution for quasi-stable ideals based on Pommaret bases. That resolution can be seen as a generalization of the famous explicit minimal resolution that Eliahou and Kervaire constructed in [7] for stable monomial ideals. Eliahou and Kervaire's resolution has certain features that allow us to consider it as part of a general framework. Particularly important are the facts that it arises as a cone resolution [5, 11] and that it has a cellular structure [13]. In [1] the authors show that Pommaret-Seiler resolution also arises as a cone resolution. We proof here that this resolution has also a cellular structure, hence showing that Pommaret-Seiler resolution is in fact a generalization of Eliahou and Kervaire's in a deep sense and can also be studied in a general framework within the theory of monomial resolutions. The cellular structure of the Pommaret-Seiler resolution suggests an algorithm for its construction and minimization. This algorithm is based on the monomial completion algorithm in [14] and the construction of a topological sorting on the graph associated to the Pommaret basis of the ideal.

1. POMMARET-SEILER RESOLUTION

Let $\mathcal{P} = \mathbf{k}[x_1, \dots, x_n]$. Any polynomial submodule of $\mathcal{M} \subseteq \mathcal{P}^m$ has a Pommaret basis, and this defines a resolution of $\mathcal{M}$, which we call *Pommaret-Seiler resolution* [14]:

Theorem 1.1 (Th. 6.1 in [14]). *Let $\mathcal{H}$ be a Pommaret basis of the polynomial submodule $\mathcal{M} \subseteq \mathcal{P}^m$. If we denote by $\beta_0^{(k)}$ the number of generators $h \in \mathcal{H}$ such that the class of their leading term* $\mathrm{cls}(le_< h) = k$ *and set* $d = \min\{k|\beta_0^{(k)} > 0\}$, *then $\mathcal{M}$ possesses a finite free resolution* $0 \longrightarrow \mathcal{P}^{t_{n-d}} \longrightarrow \cdots \longrightarrow \mathcal{P}^{t_0} \longrightarrow \mathcal{M} \longrightarrow 0$ *where the rank of the modules are given by* $t_i = \sum_{k=1}^{n-i} \binom{n-k}{i} \beta_0^{(k)}$

This resolution can be explicitly written as a complex. In the case of monomial ideals the expression for the differential is particularly compact. Let I be a quasi-stable monomial ideal and

$\mathcal{H} = \{h_1, \dots, h_s\}$ its Pommaret basis. For each $h_\alpha \in \mathcal{H}$ and any non-multiplicative variable $x_k \in \bar{\mathcal{X}}_P(h_\alpha)$ there exists a unique index $\Delta(\alpha, k)$ and a unique term $t_{\alpha;k} \in \mathbf{k}[\mathcal{X}_P(h_{\Delta(\alpha;k))}]$ such that $x_k h_\alpha = t_{\alpha;k} h_{\Delta(\alpha;k)}$. With this notation we have the following expression for the diferential of the Pommaret-Seiler resolution of I:

$$\delta(w_\alpha \otimes v_{\mathbf{k}}) = \sum_{j=1}^{i} (-1)^{i-j} (x_{k_j} w_\alpha - t_{\alpha,j} w_{\Delta(\alpha,k_j)}) \otimes v_{\mathbf{k}_j}$$

The generators of $\mathcal{H}$ can be organized as a directed acyclic graph, the P-graph of I. Despite not being minimal in general, one can immediately read off the Pommaret-Seiler resolution, without further computations, several important invariants of I. Pommaret-Seiler resolution is minimal iff I is stable, and then it coincides with the Eliahou-Kervaire resolution so it is a generalization. One can ask whether this generalization applies also in a deeper sense i.e. if important features of Eliahou-Kervaire resolution are also applied to Pommaret-Seiler. One such feature is the fact that the Eliahou-Kervaire resolution arises as a mapping cone resolution. This was proven in [5]. Herzog and Takayama describe study mapping cone resolutions in [11] and give a closed form for their differentials in the case that the ideal has linear quotients and a regular decomposition function. This good class of mapping cone resolutions are called resolutions *of Herzog-Takayama type*. Eliahou-Kervaire resolution is of Herzog-Takayama type [11].

In Theorem 7.4 in [1] the authors show that Pommaret-Seiler resolution arises also as a cone resolution. We will show now that any quasi-stable ideal I has linear quotients with respect to its Pommaret basis $\mathcal{H}$ and that a generalization of the index $\Delta(\alpha, k)$ described above provides a regular decomposition function. This implies that Pommaret-Seiler resolution is of Herzog-Takayama type.

Let I be a quasi-stable monomial ideal. Denote by $M(I)$ the set of monomials in I, $G(I)$ the set of minimal generators of I and $\mathcal{H}(I)$ the Pommaret basis of I whose elements are ordered by a P-ordering. Let $m \in M(I)$ be a monomial in I. We set $\Delta(m) = h_j$ if j is the largest element of $\mathcal{H}(I)$ such that $m = t_m h_j$ where $t_m \in \mathbf{k}[\mathcal{X}(h_j)]$. Observe that $\Delta(h_i x_j) = \Delta(i, k)$ and $\frac{m}{\Delta(i,k)} = t_{\alpha,k}$.

Lemma 1.2 (cf [10]). *Let I be a quasi-stable ideal and $\mathcal{H} = \{h_1, \dots, h_s\}$ its Pommaret basis. Then I has linear quotients with respect to $\mathcal{H}$. In particular, $\langle h_{k+1}, \dots, h_s \rangle : h_k = \langle \bar{\mathcal{X}}(h_k) \rangle$ for all k.*

Definition 1.3 (cf. [11]). For any $m_j \in G(I) = \{m_1, \dots, m_r\}$ we define $\operatorname{set}(m_j) = \{i \in [n] | x_i \in \langle m_1, \dots, m_{j-1} \rangle : m_j\}$ A *decomposition function* with respect to $G(I)$ is an assignment $b : M(I) \to G(I)$ satifying that $\forall m \in M(I)$ we have that $m = b(m)c(m)$ with $\operatorname{set}(b(m)) \cap \operatorname{supp}(c(m)) = \emptyset$

Lemma 1.4. $\Delta(m) : M(I) \to G(I)$ *is a regular decomposition function for I with respect to $\mathcal{H}$.*

Proof. It is clear that $\frac{m}{\Delta(m)}$ is by definition made of multiplicative variables for $\Delta(m)$ and on the othe hand $\operatorname{set}(\Delta(m))$ is exactly the set of nonmultiplicative variables for $\Delta(m)$, hence $\operatorname{set}(\Delta(m)) \cap \operatorname{supp}(\frac{m}{\Delta(m)}) = \emptyset$. □

Now using lemmas 1.2 and 1.4 we have from Theorem 1.12 in [11] (Theorem 2.6 in [6]) that the mapping cone resolution of I is of Herzog-Takayama type and its differential is

$$\partial(m, \alpha) = \sum_{j_i \in \alpha} (-1)^i x_{j_i} (m; \alpha - j_i) - \sum_{j_i \in \alpha} (-1)^i \frac{x_{j_i}}{\Delta(x_{j_i} m)} (\Delta(x_{j_i} m); \alpha - j_i)$$

Wich up to notation is exactly the differential of the Pommaret-Seiler resolution. Hence the Pommaret-Seiler resolution is of Herzog-Takayama type. Observe that this is in particular a simpler way to proof that Seiler-Pommaret resolution arises as a mapping cone.

2. The cellular structure of Pommaret-Seiler resolution

J. Mermin gives in [13] a cellular structure [3] for the Eliahou-Kervaire resolution. In [8] and [6] the authors give cellular structure to resolutions of Herzog-Takayama type. The cellular structure is based in the sets $\mathrm{ch}(m, \alpha, \sigma) = \mathrm{conv}(m, \Delta(x_{\sigma_1} m), \dots, \Delta(x_{\sigma_p} .. x_{\sigma_1} m))$, where σ is a permutation of α, conv is the convex hull and $\Delta(x_{\sigma_2} x_{\sigma_1} m)$ is a shorthand for $\Delta(x_{\sigma_2} \Delta(x_{\sigma_1} m))$ and so on. Using these sets we describe the cellular structure of the Pommaret-Seiler resolution as given by the cells

$$U(m, \alpha) = \bigcup_{\sigma \text{ permutation of } \alpha} \mathrm{ch}(m, \alpha, \sigma) = \mathrm{ch}(m, \mathrm{set}(m))$$

The differential for this structure is induced by the differential in the Pommaret-Seiler resolution. With this cellular construction we have that

Theorem 2.1. *If I is a quasi-stable ideal then the Pommaret-Seiler resolution of I is cellular and supported on a regular CW-complex.*

3. Algorithms

The fact that the Pommaret-Seiler resolution I is cellular and that its cellular structure can be obtained directly from the P-ordered Pommaret basis of I suggests an algorithm for the construction of the resolution based on the construction of the P-graph of I. The algorithm we propose has three steps: 1) Construct the P-graph of I, by a transformation of the monomial completion algorithm in [14]. 2) Provide the P-graph of I with a valid P-order. 3) Output the data in the P-graph as a resolution or CW-complex following the constructed P-order.

Algorithm 2 in [14] completes any finite set of monomials to the Pommaret basis of the ideal containing these monomials. We can transform this algorithm so that we construct the P-graph of I at the same time as we construct its Pommaret basis. This is done via book-keeping of the involutive divisors used when rejecting candidates of nonmultiplicative products of the elements of the provisional basis in step 3 of that algorithm, i.e. the step in which the provisional basis is (eventually) increased. This book-keeping in fact stores the new edges that we add to the P-graph in each step. The vertices are just the generators of the Pommaret basis that we are constructing. Once the P-graph is constructed (which is unique for each quasi-stable ideal) we can obtain a cellular structure for the Pommaret-Seiler resolution just by giving a topological order in P. This is no longer unique, so that we have several possibilities for the cellular structure, cf. [6]. The construction of a topological order in a directed acyclic graph $G = (V, E)$ is linear in $|V| + |E|$, see [12]. So this step can be considered as a post-processing of the construction of the P-graph. Finally, the last step of the algorithm is linear on the size of the resolution. It is a rewriting of the data in the topologically sorted P-graph.

Since the Pommaret resolution is supported on a CW-complex, we can adapt standard reduction techniques or discrete Morse theory to minimize it and obtain the minimal free resolution for this kind of ideals.

REFERENCES

[1] M. Albert, M. Fetzer, E. Sáenz-de-Cabezón, W.M. Seiler, *On the free resolution induced by a Pommaret basis*, submitted (2013)

[2] I. Bermejo, P. Gimenez, *Saturation and Castelnuevo-Mumford regularity*, Journal of Algebra 303:592-617 (2006)

[3] D. Bayer, B. Sturmfels, *Cellular resolutions of monomial modules*, J. Reine Angew. Math. 543:147-168 (1998)

[4] G. Cavligia, E.Sbarra, *Characteristic-free bounds for the Castelnuovo-Mumford regularity*, Compos. Math. 141:1365-1373 (2005)

[5] H. Charalambous, G. Evans, *Resolutions obtained by iterated mapping cones*, Journal of Algebra 176:750-754 (1995)

[6] A. Dochtermann, F.Mohammadi, *Cellular resolutions from mapping cones*, arXiv:1311.4599

[7] S. Eliahou and M. Kervaire, *Minimal resolutions of some monomial ideals*, Journal of Algebra 129:1-25 (1990)

[8] A. Goodarzi, Cellular structure for the Herzog-Takayama resolution, arXiv:1305.4302

[9] J. Herzog, D. Popescu, and M. Vladoiu, *On the Ext-modules of ideals of Borel type*, Commutative Algebra, Contemp. Math. 331: 171-186 (2003)

[10] A. Hashemi, M. Schweinfurter, W.M. Seiler, *Quasi-stability versus genericity*, CASC 2012, Lecture Notes in Computer Science 7442:172-184 (2012)

[11] J. Herzog, Y. Takayama, *Resolutions by mapping cones*, Homology, Homotopy and Applications 4(2):277-294 (2002)

[12] A.B. Kahn, *Topological sorting of large networks*, Communications of the ACM 5(11):558-562 (1962)

[13] J. Mermin, *The Eliahou-Kervaire resolution is cellular*, Journal of Commutative Algebra 2(1):55-78 (2010)

[14] W. M. Seiler, *A combinatorial approach to involtion and δ-regularity II: Structure analysis of polynomial modules with Pommaret bases*, Applicable Algebra in Engineering Communication and Computing 20:261-338 (2009)

Universidad de La Rioja
E-mail address: `eduardo.saenz-de-cabezon@unirioja.es`

A CRITICAL SET OF REVOLUTION SURFACE PARAMETRIZATIONS

J. RAFAEL SENDRA, DAVID SEVILLA, AND CARLOS VILLARINO

ABSTRACT. Given the classical rational parametrization of a surface of revolution, generated by rotating a rational curve around the z-axis, we determine a superset containing all the possible points of the surface non-reachable by the parametrization; that is a critical set of the parametrization.

1. INTRODUCTION

In some applications of algebraic surfaces, the use of their rational parametric forms to solve certain problems is only meaningful when certain properties are satisfied. For example, in order to intersect two surfaces, one given by its implicit equation and the other by a rational parametrization, substitution of the latter into the former will not provide all the points in the intersection if the parametrization is not surjective (or *normal* as called in this context [2, 3, 5]) and any point outside its image happens to lie in the intersection.

The problem of deciding whether a given surface parametrization is normal can be solved computationally by applying elimination techniques, but this is in general hindered by efficiency issues. On the other hand, for certain types of surfaces it is indeed possible to characterize the set of missing points; in particular, one can compute a *critical set*, that is, a proper closed subset of the surface that contains them. This problem has been analyzed by the authors in [7] and [6] for ruled surfaces and for parametrizations without projective base points. This article solves the problem for surfaces of revolution.

As we show later, the critical set that we calculate is parametrizable (it is a union of lines, circles, and possibly a point), so the algebraic surface can be covered by a union of finitely many parametrizations: the initial two-dimensional and several one-dimensional ones.

In the sequel, let $\mathcal{C}$ be a rational curve (called *rotation curve*) in the (y, z)-plane parametrized by $r(t) = (0, p(t), q(t))$, where $p(t), q(t) \in \mathbb{C}(t)$. Also let $\mathcal{S}$ be the surface of revolution generated by rotating $\mathcal{C}$ around the z-axis. For simplicity in the exposition we will assume that $\mathcal{C}$ is not a line parallel to the y axis, and hence $\mathcal{S}$ is not a plane. The classical parametrization of $\mathcal{S}$, obtained from $r(t)$, is

$$\mathcal{P}(s,t) = \left(\frac{2s}{1+s^2}\, p(t), \frac{1-s^2}{1+s^2}\, p(t), q(t) \right).$$

We denote any critical set of $\mathcal{P}$ by $\operatorname{Crit}(\mathcal{P})$.

A complete version of this extended abstract will be submitted to a journal.

2. MAIN RESULT

Let $\mathcal{P}(s, t)$, $\mathcal{C}$ and $\mathcal{S}$ be as in Section 1. Let $f(y, z)$ be the defining polynomial of the rotation curve $\mathcal{C}$. In [4] a description of the defining polynomial of $\mathcal{S}$ is given in terms of f. Collecting terms of odd and even degree in y we can write $f(y, z)$ as $f(y, z) = A(y^2, z) + yB(y^2, z)$.

The implicit equation of $\mathcal{S}$ depends on whether B is zero or not (i.e. f is symmetric with respect to the z-axis or not):

- $F(x, y, z) = A(x^2 + y^2, z)$ in case that $B = 0$.
- $F(x, y, z) = A^2(x^2 + y^2, z) - (x^2 + y^2)B^2(x^2 + y^2, z)$ in other case.

We consider now the rational curve $\mathcal{C}^s$ (called *mirror curve of* $\mathcal{C}$) defined as

$$\mathcal{C}^s = \{(0, -y, z) \in \mathbb{C}^3 \,/\, (0, y, z) \in \mathcal{C}\}.$$

Its implicit equation is $0 = g(y, z) = f(-y, z)$ and it is parametrized as $\gamma(s) = (0, -p(s), q(s))$. When $\mathcal{C}$ is not symmetric with respect to the z-axis, $\mathcal{C}^s$ is not reachable by $\mathcal{P}$ as we will see.

We represent by $\mathcal{C}_{\alpha,c}$ the circle of radius α in the plane $z = c$ centered at $(0, 0, c)$:

$$\mathcal{C}_{\alpha,c} = \{(x, y, z) \in \mathbb{C}^3 \,/\, x^2 + y^2 = \alpha^2, z = c\}.$$

In the next lemma we study the level curves of $\mathcal{S}$.

Lemma 2.1. *The intersection of $\mathcal{S}$ with the plane $z = c$ is either empty, or a finite union of circles $\mathcal{C}_{\alpha,c}$ with $\alpha \neq 0$, or the pair of lines $\{x \pm i\,y = 0,\ z = c\}$. Moreover, if $(x_0, y_0, z_0) \in \mathcal{S}$ where $x_0^2 + y_0^2 = \alpha^2 \neq 0$, then $\mathcal{C}_{\alpha,z_0} \subset \mathcal{S}$.*

When a point $P \in \mathcal{C}$ rotates around the z-axis it generates a circle in $\mathcal{S}$ except when P belongs to the rotation axis. In the following lemmas we analyze these cases.

Lemma 2.2. *Let $P = r(t_0) = (0, p(t_0), q(t_0))$ with $p(t_0) \neq 0$, i.e. $P \in \mathcal{C}$ is reachable by $r(t)$ and is not on the revolution axis. Then $\mathcal{C}_{p(t_0),q(t_0)}$, obtained by rotating P around the z-axis, is reachable by $\mathcal{P}$, except possibly the symmetric point $P_s = (0, -p(t_0), q(t_0)) \in \mathcal{C}^s$.*

Lemma 2.3. *The following statements are equivalent:*

(1) $(0, 0, z_0) \in \mathcal{C}$,

(2) *$\mathcal{S}$ contains the lines $\{x \pm i\,y = 0, z = z_0\}$.*

Moreover,

(i) *If $(0, 0, z_0) \in \mathcal{C}$, the lines $\{x \pm i\,y = 0, z = z_0\}$ are not reachable by $\mathcal{P}$, except possibly the point $(0, 0, z_0)$.*

(ii) *If $(x_0, y_0, z_0) \in \mathcal{S}$ with $x_0^2 + y_0^2 = 0$, then $(0, 0, z_0) \in \mathcal{C}$.*

(iii) *If $(x_0, y_0, z_0) \in \mathcal{S}$ with $x_0^2 + y_0^2 = 0$, then $\{x \pm i\,y = 0, z = z_0\} \subset \mathcal{S}$.*

Lemma 2.4. *Let $(x_0, y_0, z_0) \in \mathcal{S}$. Then $P^+ = (0, \sqrt{x_0^2 + y_0^2}, c)$ or $P^- = (0, -\sqrt{x_0^2 + y_0^2}, c)$ belongs to $\mathcal{C}$.*

Lemma 2.5. *Let $\mathcal{C}_{\alpha,c} \subset \mathcal{S}$, with $\alpha \neq 0$, and let $P_1 = (0, \alpha, c)$, $P_2 = (0, -\alpha, c)$. The following statements are equivalent:*

(1) *$\mathcal{C}_{\alpha,c}$ contains at least one point reachable by $\mathcal{P}$.*

(2) *$\mathcal{C}_{\alpha,c}$ is reachable by $\mathcal{P}$ except, at most, one of the points P_i.*

(3) *One of the points P_i is reachable by $r(t)$.*

The next theorem describes a critical set of the surface $\mathcal{S}$. This description is general; nevertheless, as we will see in the proof, in some situations the critical set can be optimized (see Remark 2.7). We speak about the critical point of the curve parametrization $r(t)$ in the sense of [5]: the only point on the Zariski closed curve that might not be reachable by $r(t)$.

Theorem 2.6. *A critical set for $\mathcal{P}$ is*

$$\mathrm{Crit}(\mathcal{P}) = \bigcup_{i=1}^{k} \{x \pm i\,y = 0, z = \lambda_i\} \cup \mathcal{C}^s \cup \mathcal{C}_{\rho,c} \quad \textit{where}$$

- $\mathcal{C} \cap \{x = y = 0\} = \{(0,0,\lambda_i)\}_{i=1,\dots,k}$*,*
- $P^* = (0, \rho, c)$*, with* $\rho \neq 0$*, is the critical point of the parametrization* $r(t)$*.*

Proof. Let $N = (x_0, y_0, z_0) \in \mathcal{S} \setminus \mathcal{P}(\mathbb{C}^2)$. If $x_0^2 + y_0^2 = 0$, by Lemma 2.3, $N \in \{x \pm i\,y = 0, z = z_0\} \subset \mathrm{Crit}(\mathcal{P})$. Let $x_0^2 + y_0^2 = \alpha^2 \neq 0$. By Lemma 2.1, $\mathcal{C}_{\alpha,z_0} \subset \mathcal{S}$, and by Lemma 2.4 $P^+ = (0, \alpha, z_0)$ or $P^- = (0, -\alpha, z_0)$ belongs to $\mathcal{C}$. We now distinguish two cases:

(1) Assume $P^{\pm} \in \mathcal{C}$. Note that, by [5, Theorem 2], al least one of them is reachable by $r(t)$, and hence by $\mathcal{P}(s,t)$. Assume w.l.o.g. that P^+ is reachable by $r(t)$. By Lemma 2.5, $\mathcal{C}_{\alpha,z_0}$ is reachable by $\mathcal{P}$ with the possible exception of P^-. Since $N \in \mathcal{C}_{\alpha,z_0}$ and it is non-reachable, then $P^- = N$. Moreover, $P^* = P^-$. Thus, $N \in \mathcal{C}^s \subset \mathrm{Crit}(\mathcal{P})$.

(2) Assume either P^+ or P^- belong to $\mathcal{C}$. Assume also w.l.o.g. that $P^+ \in \mathcal{C}$:
   (a) If $P^+ = r(t_0)$, by Lemma 2.2, $\mathcal{C}_{\alpha,z_0}$ is reachable except at $P^- = N$. So, $N \in \mathcal{C}^s \subset \mathrm{Crit}(\mathcal{P})$.
   (b) If P^+ is not reachable by $r(t)$, by Lemma 2.5, $N \in \mathcal{C}_{\alpha,z_0} \subset \mathrm{Crit}(\mathcal{P})$. □

Remark 2.7. Taking into account the reasoning in the last proof, we derive the following process to optimize the critical set.

(1) Let $\mathrm{Crit}(\mathcal{P}) = \emptyset$.
(2) Compute the intersections of $\mathcal{C}$ with the z-axis. If $\mathcal{C} \cap \{x = y = 0\} = \{(0,0,\lambda_i)\}_{i=1,\dots,k}$ then include $\bigcup_{i=1}^{k} \{x \pm i\,y = 0, z = \lambda_i\}$ in $\mathrm{Crit}(\mathcal{P})$.
(3) Check whether $\mathcal{C}$ is symmetric with respect to the z-axis.
   (a) If $\mathcal{C}$ is symmetric check whether $r(t)$ is normal. If $r(t)$ is normal then RETURN $\mathrm{Crit}(\mathcal{P})$, else include the missing point of $r(t)$ in $\mathrm{Crit}(\mathcal{P})$ and RETURN $\mathrm{Crit}(\mathcal{P})$.
   (b) If $\mathcal{C}$ is not symmetric then include $\mathcal{C}^s$ in $\mathrm{Crit}(\mathcal{P})$ and check whether $r(t)$ is normal. If $r(t)$ is normal then RETURN $\mathrm{Crit}(\mathcal{P})$, else
      (i) compute the missing point $(0, a, b)$ of $r(t)$ and if $a = 0$ then RETURN $\mathrm{Crit}(\mathcal{P})$,
      (ii) if $(0, -a, b) \in \mathcal{C}$ then RETURN $\mathrm{Crit}(\mathcal{P})$, else include $\mathcal{C}_{a,b}$ in $\mathrm{Crit}(\mathcal{P})$ and RETURN $\mathrm{Crit}(\mathcal{P})$.

Remark 2.8. To check the normality of $r(t)$ one can apply Theorem 2 in [5]. To check symmetry one can use the ideas in [1] or compute the implicit equation $f(y,z)$ of $\mathcal{C}$ and check whether $f(-y,z) = f(y,z)$.

3. Examples

We illustrate our results with two examples.

Example 3.1. The *pear–shaped curve* $\mathcal{C}$ given by $x = z^2 - y^3(1-y) = 0$ is parametrized as

$$r(t) = (0, p(t), q(t)) = \left(0, \frac{16t^2 + 8t + 1}{17t^2 + 32t + 145}, -\frac{64t^4 + 816t^3 + 588t^2 + 145t + 12}{289t^4 + 1088t^3 + 5954t^2 + 9280t + 21025}\right).$$

It holds that $\mathcal{C} \cap \{x = y = 0\} = \{(0,0,0)\}$, $\mathcal{C}$ is not symmetric with respect to the z-axis, and $r(t)$ is not normal (the point $\left(0, \frac{16}{17}, -\frac{64}{289}\right)$ is not reachable). Taking into account Remark 2.7, a critical set for the usual parametrization of the revolution surface generated by $r(t)$ is

$$\mathrm{Crit}(\mathcal{P}) = \{x \pm \, i\, y = 0, z = 0\} \cup \mathcal{C}^s \cup \mathcal{C}_{\frac{16}{17},-\frac{64}{284}}.$$

On the other hand we can rotate $\mathcal{C}$ around the y-axis; for simplicity, consider the curve obtained by rotating $\mathcal{C}$ an angle $\pi/2$ in the yz-plane. The new curve, of shape similar to that of $\mathcal{C}$, has equations $\{x = 0, y^2 = z^3(1-z)\}$, and can be parametrized as $r(t) = (0, q(t), p(t))$. In this case $\mathcal{C} \cap \{x = y = 0\} = \{(0,0,0), (0,0,1)\}$, $\mathcal{C}$ is symmetric with respect to the z-axis, and $r(t)$ is not normal, being $\left(0, -\frac{64}{289}, \frac{16}{17}\right)$ its non-reachable point. Then

$$\mathrm{Crit}(\mathcal{P}) = \{x \pm \, i\, y = 0, z = 0\} \cup \{x \pm \, i\, y = 0, z = 1\} \cup \left\{ \left(0, -\frac{64}{289}, \frac{16}{17}\right) \right\}.$$

Example 3.2. *Kulp's quartic* $\mathcal{C}$ has equations $\{x = 0, y^2(1+z^2) = 1\}$ and parametrization

$$r(t) = \left(0, -\frac{3t^2+4t+1}{5t^2+4t+1}, \frac{2(2t+1)t}{3t^2+4t+1}\right).$$

In this case $\mathcal{C} \cap \{x = y = 0\} = \{\emptyset\}$, $\mathcal{C}$ is symmetric with respect to the z-axis, and $r(t)$ is not normal (the point $\left(0, -\frac{3}{5}, \frac{4}{3}\right)$ is not reachable). Then $\mathrm{Crit}(\mathcal{P}) = \left\{ \left(0, -\frac{3}{5}, \frac{4}{3}\right) \right\}$.

Acknowledgments

The authors are supported by the Spanish *Ministerio de Economía y Competitividad* under the Project MTM2011-25816-C02-01. The first and third authors are members of the Research Group ASYNACS (Ref. CCEE2011/R34).

References

[1] J.G. Alcázar, C. Hermoso, G. Muntingh. Detecting Symmetries of Rational Plane and Space Curves. *Computer Aided Geometric Design*, to appear, 2014.

[2] C. Andradas, T. Recio. Plotting missing points and branches of real parametric curves. *Appl. Algebra Engrg. Comm. Comput.*m 18(1–2):107–126, 2007.

[3] X. S. Gao, S.-C. Chou. On the normal parameterization of curves and surfaces. *Internat. J. Comput. Geom. Appl.*, 1(2):125–136, 1991.

[4] F. San Segundo, J. R. Sendra. Offsetting Revolution Surfaces. *ADG 2008, LNCS 6301 (T. Sturm and C. Zengler Eds.)*, pp. 179–188. Springer-Verlag Berlin Heidelberg (2011) ISBN: 978-3-642-21045-7.

[5] J. R. Sendra. Normal parametrizations of algebraic plane curves. *J. Symbolic Comput.*, 33(6):863–885, 2002.

[6] J. R. Sendra, D. Sevilla, and C. Villarino. Covering of surfaces parametrized without projective base points. Accepted in Proc. ISSAC 2014.

[7] J. R. Sendra, D. Sevilla, and C. Villarino. Some results on the surjectivity of surface parametrizations. Accepted in a LNCS volume, 2014.

Centro Universitario de Mérida, Av. Santa Teresa de Jornet 38, E-06800, Mérida, Badajoz, Spain
E-mail address: sevillad@unex.es

Dpto. de Matemáticas, Universidad de Alcalá, E-28871 Madrid, Spain, Members of the Research Group ASYNACS (Ref. CCEE2011/R34)
E-mail address: rafael.sendra@uah.es; carlos.villarino@uah.es

PERTURBATION RESULTS ON POLYNOMIALS ZERO-LOCI

MARIA-LAURA TORRENTE

ABSTRACT. Let f, g be complex multivariate polynomials. We bound the euclidean distance of points belonging to the zero-loci of f and g in terms of the Bombieri norm $\|f - g\|$.

INTRODUCTION

We address the problem of evaluating how much the zero-locus of a multivariate complex polynomial varies, if some perturbation on the polynomial coefficients is permitted. Our main result (see Theorem 2.2) is local and is a generalization of the paper [1], where the univariate case is considered. The proof makes is based on Walsh Contraction Principle (see Proposition 2.1) and makes use of Bombieri's scalar product properties. We highlight here our work, omitting the proofs due to length reasons. Having in mind applications, the study of the problem over the reals seems to be a case of relevant interest. This is an ongoing research joint with M. C. Beltrametti.

1. BOMBIERI–WEYL'S NORM

We let $x_1, \ldots, x_n$ be indeterminates. The multivariate polynomial ring with complex coefficients $\mathbb{C}[x_1, \ldots, x_n]$ is denoted by P. We choose a new indeterminate x_0, also called *homogenizing indeterminate*, and denote the polynomial ring $\mathbb{C}[x_0, x_1, \ldots, x_n]$ by $\overline{P}$.

The homogenization and dehomogenization of a polynomial meet some properties for which we refer to [7, Definition 4.3.1 and Proposition 4.3.2]. Let f be a polynomial of P and let F be a homogeneous polynomial of $\overline{P}$. Let $f = f_d + \ldots + f_0$ be the decomposition of f into its homogeneous components, where each $f_i \in P$ is homogeneous of degree i. The *homogenization of f with respect to* x_0 is the polynomial $f^{\mathrm{hom}} = f_d + x_0 f_{d-1} + \ldots + x_0^d f_0 \in \overline{P}$. For the zero polynomial, we set $0^{\mathrm{hom}} = 0$. The *dehomogenization of F w.r.t.* x_0 is the polynomial $F^{\mathrm{deh}} = F(1, x_1, \ldots, x_n) \in P$.

Given $\boldsymbol{\alpha} = (\alpha_0, \ldots, \alpha_n) \in \mathbb{N}^{n+1}$, we denote by $|\boldsymbol{\alpha}|$ the number $\alpha_0 + \ldots + \alpha_n$ and by $\boldsymbol{\alpha}!$ the number $\alpha_0! \ldots \alpha_n!$.

Definition 1.1. (See [3]) Let $F = \sum_{|\boldsymbol{\alpha}|=d} c_{\boldsymbol{\alpha}} x_0^{\alpha_0} \ldots x_n^{\alpha_n}$ be a degree d homogeneous polynomial of $\overline{P}$ and let f be a degree d polynomial of P.

a) The *Bombieri norm* of F is defined as

$$\|F\|_{(d)} = \left(\sum_{|\boldsymbol{\alpha}|=d} \frac{\alpha_0! \ldots \alpha_n!}{d!} |c_{\boldsymbol{\alpha}}|^2 \right)^{1/2}.$$

b) The *Bombieri norm* of f is defined as the Bombieri norm of the homogenization of f, that is, $\|f\|_{(d)} = \|f^{\mathrm{hom}}\|_{(d)}$.

The following scalar product, known as Bombieri's scalar product, is canonically associated to Bombieri's norm (see [4]).

Definition 1.2. Let $F = \sum_{|\boldsymbol{\alpha}|=d} c_{\boldsymbol{\alpha}} x_0^{\alpha_0} \dots x_n^{\alpha_n}$ and $G = \sum_{|\boldsymbol{\alpha}|=d} c'_{\boldsymbol{\alpha}} x_0^{\alpha_0} \dots x_n^{\alpha_n}$ be homogeneous polynomials of $\overline{P}$ of degree d, and let f, g be polynomials of P of degree d. Then:[1]

a) The *Bombieri scalar product* of F and G is defined as

$$(F, G)_{(d)} = \sum_{|\boldsymbol{\alpha}|=d} \frac{\alpha_0! \dots \alpha_n!}{d!} c_{\boldsymbol{\alpha}} \overline{c'_{\boldsymbol{\alpha}}}$$

b) The *Bombieri scalar product* of f and g is defined as the Bombieri scalar product of the homogenization of f and g, that is, $(f, g)_{(d)} = (f^{\text{hom}}, g^{\text{hom}})_{(d)}$.

2. The main result

Let us recall Walsh Contraction Principle (see [10], [2]), a result on the zeros of multivariate symmetric polynomials which are linear with respect to each variable. We recall that, in Walsh's terminology, a (*closed*) *circular region* of the complex plane is either a (closed) disk, or a (closed) half-plane, or the (closed) exterior of a disk.

Theorem 2.1. (Walsh's Contraction Principle) *Let $f \in \mathbb{C}[x_1, \dots, x_n]$ be a polynomial with the following properties:*

(1) *f is linear w.r.t. each variable x_i;*
(2) *f is symmetric w.r.t. the variables x_i, that is, $f(x_{\sigma(1)}, \dots, x_{\sigma(m)}) = f(x_1, \dots, x_n)$ for each order n permutation σ (equivalently, f is invariant under permutations of the variables x_i).*

Let D be a circular region of the complex plane, and assume that there are $z_1, \dots, z_n \in D$ such that $f(z_1, \dots, z_n) = 0$. Then there exists a point $y \in D$ such that $f(y, \dots, y) = 0$.

Now, let f be a polynomial of P of degree d; following standard notation, we denote by $\text{Jac}_f = (\frac{\partial f}{\partial x_1}, \dots, \frac{\partial f}{\partial x_n})$ the *Jacobian* of f. Let $g \in P$ be polynomial, with same degree d, slightly differing from f, that is, such that $\|g - f\| \leq \varepsilon$, for a given positive real number ε. Let $p \in \mathbb{A}^n_{\mathbb{C}}$ be a point of the zero-locus of f, that is, $f(p) = 0$. The following theorem provides a "local" estimate for the difference between the zero-loci of f and g, that is, it gives a bound for the Euclidean norm $\|q - p\|_2$ in $\mathbb{C}^n$, where q satisfies $g(q) = 0$. The proof, that we omit for length reasons, uses the properties of Bombieri's scalar product and Theorem 2.1.

Theorem 2.2. *Let f and g be degree d polynomials of P and let $p \in \mathbb{A}^n_{\mathbb{C}}$ be a non-singular point of $f = 0$ such that $\text{Jac}_g(p)$ is a non-zero vector. Let ε be a positive real number, and suppose that $\|g - f\| \leq \varepsilon$. Then there exists a point $q \in \mathbb{A}^n_{\mathbb{C}}$ belonging to $g = 0$ such that*

$$\|q - p\|_2 \leq \frac{d(1 + \|p\|_2^2)^{d/2}}{\|\text{Jac}_g(p)\|_1} \varepsilon. \tag{1}$$

[1] For simplicity, in the sequel, the subscript $\cdot_{(d)}$ used in Bombieri's norm and in Bombieri's scalar product will be omitted; nevertheless, it should be clear that these quantities depend on the degree of the polynomials.

Furthermore, if ε *is small enough, namely if* $\varepsilon \le \frac{1}{2}\frac{\|\mathrm{Jac}_f(p)\|_1}{d(1+\|p\|_2^2)^{\frac{d-1}{2}}}$, *then*

$$\|q-p\|_2 \le \frac{2d(1+\|p\|_2^2)^{d/2}}{\|\mathrm{Jac}_f(p)\|_1}\varepsilon. \tag{2}$$

Let us add a few comments. First, note that in the univariate case Theorem 2.2 gives back Beauzamy's results [1, Theorem 1]. Moreover, as in [1], estimates (1) and (2) of Theorem 2.2 are invariant under scalar multiplication. In fact, by multiplying the polynomials f and g by the same non-zero constant λ, we observe that the quantities ε, $\|\mathrm{Jac}_g(p)\|_1$, and $\|\mathrm{Jac}_f(p)\|_1$ result in a multiplication by λ, so inequalities (1) and (2) are not modified. Further, Theorem 2.2 applies to non-singular points of $f = 0$: we plan to avoid this condition to get a "singular" version of the result.

Example 2.3. In the affine plane $\mathbb{A}^2_{(x,y)}(\mathbb{R})$ consider the two cubic curves of equations $f = 0$ and $g = 0$, where $f = x^2 + y^3 + y - 2$ and $g = x^2 + 1.1y^3 + 1.2y - 2.2$ (see Figure 1). Note that the coefficients of the polynomial g "slightly" differ from the corresponding coefficients of the polynomial f, and this leads to consider the curve $g = 0$ as a "small" perturbation of the curve $f = 0$. In order to quantify the size of the perturbation, we measure the difference between f and g by computing the Bombieri norm $\|g - f\| = \frac{1}{10}\sqrt{10/3} \approx 0.18$.

We consider two points of the curve $f = 0$, namely $p_1 = (0, 1)$ and $p_2 = (1, 0)$, and we compute estimate (1) of Theorem 2.2 in both cases. In the first case, the value of the upper bound is equal to $4\sqrt{15}/45 \approx 0.34$, whereas in the second case the value is $\sqrt{15}/5 \approx 0.77$. These values provide upper bounds to the roots differences $\|q-p_1\|_2$ and $\|q-p_2\|_2$, where q is a point of the curve $g = 0$. We note that, for the point p_1, the value $\varepsilon = \|g - f\| \approx 0.18$ is small enough to get estimate (2). In this case $\|q - p_1\|_2$ is bounded by $2\sqrt{15}/5 \approx 1.55$.

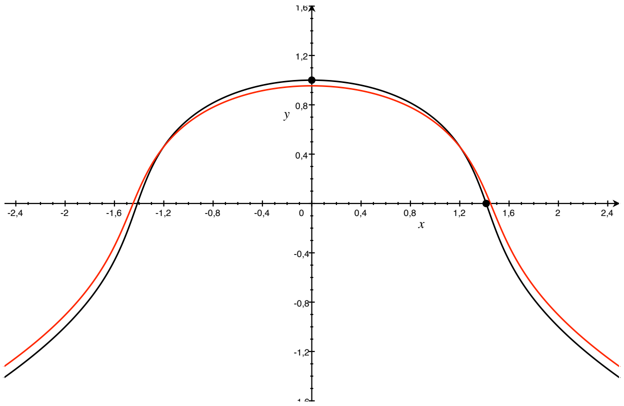


FIGURE 1. The two curves $f = 0$ (black) and $g = 0$ (red).

3. PROBLEMS AND MOTIVATIONS

Let us briefly sketch how our results can be applied in a case of special interest, that is, the Hough transform technique. The Hough transform is a pattern recognition technique for the automated recognition of curves in images (see, e.g., [5], [6] and [8] for full details). In this context, consider a family $\mathcal{F}$ of real curves in the image plane $\mathbb{A}^2_{(x,y)}(\mathbb{R})$ of equation

$$f_\lambda(x,y) = \sum_{i,j=0}^{d} x^i y^j g_{ij}(\lambda), \quad i+j \leq d, \tag{3}$$

where $f_\lambda(x,y) \in \mathbb{R}[x,y]$ is a degree d polynomial and $\lambda := (\lambda_1,\ldots,\lambda_t) \in \mathcal{U} \subseteq \mathbb{R}^t$, for some euclidean open set $\mathcal{U}$, is a tuple of independent parameters. The *Hough transform* $\Gamma_p(\mathcal{F})$ *of a point* $p \in \mathbb{A}^2_{(x,y)}(\mathbb{R})$ *with respect to* $\mathcal{F}$ is the hypersurface in the affine parameter space $\mathbb{R}^t$ whose equation is obtained by evaluating (3) in p and letting λ vary.

The core of the recognition algorithm based on the Hough transforms is to count how many hypersurfaces $\Gamma_p(\mathcal{F})$ cross a given cell of a suitable discretization of the parameter space $\mathbb{R}^t$. The value λ of the center of the cell which counts the maximum number of crossings is then used to construct and detect the recognized curve $f_\lambda(x,y)=0$ (see [9]). Since both the coordinates of the points p and the values of the parameters λ are known up to a limited accuracy, a relevant issue is to understand how the zero-loci of the polynomials $\Gamma_p(\mathcal{F})$ and $f_\lambda(x,y)$ vary for small perturbations of p and λ respectively. Clearly enough, Theorem 2.2 leads to think to some perturbation results to be used to this end. On the other hand, this theorem is based on Walsh Contraction Principle which does not hold over $\mathbb{R}$. Motivated by the pattern recognition technique highlighted above, we aim to find a “real” version of Theorem 2.2 holding true over the field $\mathbb{R}$ of the real numbers.

REFERENCES

[1] B. Beauzamy, How the Roots of a Polynomial Vary with its Coefficients: a Local Quantitative Result, Canad. Math. Bull. **42**(1) (1999), 3–12.

[2] B. Beauzamy, Finding the Roots of Polynomial Equations: an Algorithm with Linear Command, Rev. Mat. Complut. XIII(2) (2000), 305–323.

[3] B. Beauzamy, E. Bombieri, P. Enflo, H. L. Montgomery, Products of polynomials in Many Variables, J. Number Theory, **36** (1990), 219–245.

[4] B. Beauzamy, J. Dégot, Differential Identities, Trans. Am. Math. Soc. **347**(7) (1995), 2607–2619.

[5] M. C. Beltrametti, A. M. Massone and M. Piana, Hough transform of special classes of curves, SIAM J. Imaging Sci. **6**(1) (2013), 391–412.

[6] M. C. Beltrametti and L. Robbiano, An algebraic approach to Hough transforms, J. Algebra **371** (2012), 669–681.

[7] M. Kreuzer, L. Robbiano, *Computational Commutative Algebra 2*, Springer-Verlag, 2005.

[8] A. M. Massone, A. Perasso, C. Campi and M. C. Beltrametti, Profile detection in medical and astronomical imaging by mean of the Hough transform of special classes of curves, preprint, 2013.

[9] M. Torrente and M. C. Beltrametti, Almost vanishing polynomials and an application to the Hough transform, J. Algebra Appl. (to appear).

[10] J. L. Walsh, On the Location of the Roots of Certain Types of Polynomials, Trans. Am. Math. Soc. **12** (1922), 163–180.

M. Torrente, Dipartimento di Matematica, Università di Genova, Via Dodecaneso 35, I-16146 Genova, Italy.

E-mail address: torrente@dima.unige.it

RING STRUCTURE OF SPLINES ON TRIANGULATIONS

NELLY VILLAMIZAR

INTRODUCTION

For a triangulated region Δ in $\mathbb{R}^2$, we consider the space $C^r(\Delta)$ of piecewise polynomial functions that are continuously differentiable of order r (C^r functions) on Δ. These functions are called splines, and they have many practical applications including the finite element method for solving differential equations. They are also very useful for modeling surfaces of arbitrary topology and are a widely recognized tool in isogeometric analysis, and free-form representation in Computer Aided Geometric Design.

Besides the interest that the space of splines has for applications, for every $r \geq 0$, the set $C^r(\Delta)$ forms a ring under pointwise multiplication. It was proved that, as a ring, $C^0(\Delta)$ is a quotient of the Stanley–Reisner ring A_Δ of Δ [2]. Since $C^{r+1}(\Delta) \subset C^r(\Delta)$, this result implies that there is a descending chain of subrings contained in A_Δ. We use a local characterization to study the ring structure of those elements of the Stanley–Reisner ring which correspond to splines of higher-order smoothness [6], we present some results, and a conjecture for the ring structure of splines on generic triangulations.

1. STANLEY-REISNER RING ASSOCIATED TO A SPLINE SPACE

Throughout this notes Δ will denote a simplicial complex supported on a simply connected domain $|\Delta| \subset \mathbb{R}^2$, and by $C^r_k(\Delta)$ we denote the space of C^r splines (for some integer $r \geq 0$) defined on Δ of degree less than or equal to k. The dual graph G_Δ associated to Δ is the graph with vertices corresponding to the 2-cells in Δ, and edges corresponding to adjacent pairs of 2-cells. Thus, in our setting, G_Δ will be connected and its number of cycles will depend on the number of interior vertices of Δ.

For an edge τ, let $L_\tau \in \mathbb{R}[x_1, x_2]$ be the linear polynomial vanishing on τ, and $\ell_\tau \in R := \mathbb{R}[x_1, x_2, x_3]$ its homogenization. In [2], it was proved that $C^0(\Delta)$ is isomorphic to $A_\Delta / \sum_{i=1}^n Y_i - 1$ as $\mathbb{R}$-algebras, where $A_\Delta := \mathbb{R}[Y_1, \ldots, Y_n]/I_\Delta$. The number of variables corresponds to the number of vertices $v_1, \ldots, v_n$ (on the boundary and in the interior) of Δ, and I_Δ is the ideal of nonfaces of Δ, which by definition, is the ideal generated by the square-free monomials corresponding to vertex sets which are not faces of Δ, namely

$$I_\Delta = \langle Y_{i_1} \cdots Y_{i_j} : \{v_{i_1}, \ldots, v_{i_j}\} \notin \Delta \rangle.$$

The key idea for this isomorphism is to view the variables of A_Δ as Courant functions centered at the corresponding vertex i.e., $Y_i(v_j) = \delta_{ij}$ where δ_{ij} is the Kronecker delta, $i, j = 1, \ldots, n$.

Let us embed Δ in the plane $\{x_3 = 1\} \subset \mathbb{R}^3$, and form the cone $\hat{\Delta}$ over Δ with vertex at the origin, and consider the splines $C^r(\hat{\Delta})$ defined on $\hat{\Delta}$. The Stanley–Reisner ring $A_{\hat{\Delta}}$ has one variable more than A_Δ, but since that additional variable corresponds to the vertex of the cone it does not appear in any of the generators of I_Δ, hence

$$C^0(\hat{\Delta}) \cong A_\Delta. \tag{1}$$

Viewing the variables of the (affine) Stanley–Reisner ring as Courant functions gives a geometric picture of $C^0(\Delta)$; the *homogenization* allows to use tools from algebraic geometry for graded rings for studying $C^r(\Delta)$ [3–5]. Since there is a natural embedding

$$C^{r+1}(\hat{\Delta}) \hookrightarrow C^r(\hat{\Delta}) \tag{2}$$

for every $r \geq 0$, the isomorphism (1) implies that there is a descending chain of subalgebras contained in A_Δ, each corresponding to a subalgebra of splines of increasing orders of smoothness [6].

2. Local characterization and C^r-splines

Let σ_1 and σ_2, as in Fig. 1, be two triangles which meet along an edge $\tau = \sigma_1 \cap \sigma_2$. Then, if f, g are polynomials supported on (the homogenizations) $\hat{\sigma}_1$ and $\hat{\sigma}_2$ respectively, f and g meet C^r smoothly if and only if $\ell_\tau^{r+1} | (f - g)$ 1 [1]. This condition translates into a condition on the polynomials in A_Δ as follows, [6].

For each vertex v_i in Δ let us denote by (v_{i1}, v_{i2}) its coordinates. For a triangle $\sigma = \{v_i, v_j, v_k\}$, let $x_i^\sigma, x_j^\sigma, x_k^\sigma$ be the linear functions that give the barycentric coordinates of a point in $\mathbb{R}^2$ in terms of the vertices of σ. Let $X_i^\sigma, X_j^\sigma, X_k^\sigma$ be the homogenization of x_i^σ, x_j^σ and x_k^σ with respect to x_3, respectively. Define $A_\sigma := \mathbb{R}[X_i^\sigma, X_j^\sigma, X_k^\sigma]$, and let

$$B_\sigma : \mathbb{R}[x_1, x_2, x_3] \to A_\sigma \tag{3}$$

be the automorphism defined by

$$\begin{aligned} x_1 &\to v_{i1} X_i^\sigma + v_{j1} X_j^\sigma + v_{k1} X_k^\sigma \\ x_2 &\to v_{i2} X_i^\sigma + v_{j2} X_j^\sigma + v_{k2} X_k^\sigma \\ x_3 &\to X_i^\sigma + X_j^\sigma + X_k^\sigma. \end{aligned}$$

If σ_1 and σ_2 are two triangles as in Fig. 1, the change of coordinates from A_{σ_2} to A_{σ_1} is given by the map

$$B_{\sigma_2 \sigma_1} : A_{\sigma_2} \to A_{\sigma_1} \tag{4}$$

defined by

$$\begin{aligned} X_l^{\sigma_2} &\to \frac{v_{ijk}}{v_{ljk}} X_i^{\sigma_1} \\ X_j^{\sigma_2} &\to \frac{v_{lik}}{v_{ljk}} X_i^{\sigma_1} + X_j^{\sigma_1} \\ X_k^{\sigma_2} &\to \frac{v_{lji}}{v_{ljk}} X_i^{\sigma_1} + X_k^{\sigma_1}, \end{aligned}$$

where v_{ijk} denotes the determinant

$$v_{ijk} = \begin{vmatrix} v_{i1} & v_{j1} & v_{k1} \\ v_{i2} & v_{j2} & v_{k2} \\ 1 & 1 & 1 \end{vmatrix}.$$

Proposition 2.1 ([6]). *A polynomial $F \in A_\Delta$ corresponds to an element of $C^r(\Delta)$ if and only if $(X_i^{\sigma_1})^{r+1}$ divides $F|_{\sigma_1} - B_{\sigma_2\sigma_1}(F|_{\sigma_2})$, with the notation as in Fig. 1, for each interior edge $\tau = \sigma_1 \cap \sigma_2$ of Δ.*

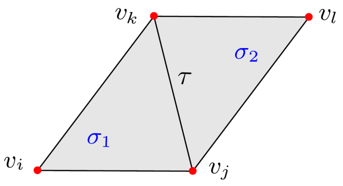


FIGURE 1. Triangles σ_1, σ_2, with $\sigma_1 \cap \sigma_2 = \tau$.

The previous condition applied to each interior edge of a given triangulation Δ yields a characterization of the elements in A_Δ which correspond to splines $C^r(\Delta)$ [6], and leads to the following result.

Proposition 2.2. *Let Δ be a 2-dimensional simplicial complex consisting of least two triangles $\sigma_1 = \{v_0, v_1, v_2\}$ and $\sigma_2 = \{v_0, v_2, v_3\}$, such that its graph G_Δ is a tree (i.e., a connected graph with no cycles). If Δ has $m+1$ vertices then*

$$C^r(\Delta) \cong \mathbb{R}[H_0, H_1, H_2, Y_3^{r+1}, \ldots, Y_m^{r+1}]/I_\Delta,$$

where

$$\begin{aligned} H_0 &= Y_0 + Y_1 + \cdots + Y_m \\ H_1 &= v_{01}Y_0 + v_{11}Y_1 + \cdots + v_{m1}Y_m \\ H_2 &= v_{02}Y_0 + v_{12}Y_1 + \cdots + v_{m2}Y_m. \end{aligned}$$

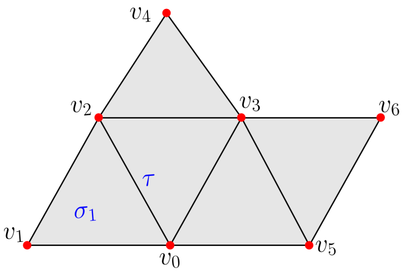


FIGURE 2. Example, Proposition 2.2.

Sketch of the proof. Let us assume Δ has only two triangles $\sigma_1 = \{v_0, v_1, v_2\}$ and $\sigma_2 = \{v_0, v_2, v_3\}$. Then, the Stanley–Reisner ring associated to Δ is $A_\Delta = \mathbb{R}[Y_0, Y_1, Y_2, Y_3]/\langle Y_1 Y_3 \rangle$. Let $F \in A_\Delta$ be the linear polynomial

$$F = a_0 Y_0 + a_1 Y_1 + a_2 Y_2 + a_3 Y_3,$$

with $a_i \in \mathbb{R}$. From Proposition 2.1, if F corresponds to an element in $C^r(\Delta)$, the difference $F|_{\sigma_1} - B_{\sigma_2\sigma_1}(F|_{\sigma_2})$ must be divisible by $(X_1^{\sigma_1})^{r+1}$, with $B_{\sigma_2\sigma_1}$ as defined in (3). Since

$$F|_{\sigma_1} - B_{\sigma_2\sigma_1}(F|_{\sigma_2}) = (a_0 - a_0)X_0^{\sigma_1} + (a_2 - a_2)X_2^{\sigma_1} + \left(a_1 - a_0 \frac{v_{123}}{v_{023}} - a_2 \frac{v_{013}}{v_{023}} - a_3 \frac{-v_{012}}{v_{023}} \right) X_1^{\sigma_1}$$

then (a_0, a_1, a_2, a_3) must be in the kernel of the matrix

$$\begin{pmatrix} -v_{123} & v_{023} & -v_{013} & v_{012} \end{pmatrix}. \tag{5}$$

This kernel is spanned by the rows of the matrix

$$\begin{pmatrix} v_{01} & v_{11} & v_{21} & v_{31} \\ v_{02} & v_{12} & v_{22} & v_{32} \\ 1 & 1 & 1 & 1 \end{pmatrix},$$

and these rows define H_0, H_1, H_2. These polynomials correspond exactly to the trivial splines ($f|_\sigma = f$ for all $\sigma \in \Delta$) on Δ, which generate the ring of polynomials R (contained in $C^r(\Delta)$). The first degree we need to consider to get not trivial splines is $r+1$. Following an analogous construction as before, it is easy to check that Y_3^{r+1}, by Proposition 2.1, corresponds to a spline in $C^r(\hat{\Delta})$ which is nontrivial. Hence, all the polynomials in the ring $\mathbb{R}[H_0, H_1, H_2, Y_3^{r+1}]/I_\Delta$ correspond to elements in $C^r(\hat{\Delta})$. The other inclusion follows from the dimension formula for $C_k^r(\Delta)$ [4],

$$\dim C_k^r(\Delta) = \binom{k+2}{2} + \binom{k+1-r}{2}.$$

For a simplicial complex Δ with $m \geq 3$ triangles, the proposition follows by applying the previous procedure recursively adding one new triangle at the time. □

Conjecture 2.3. *For a generic central configuration Δ, where G_Δ is a cycle,*

$$C^r(\hat{\Delta}) \cong \mathbb{R}[H_0, H_1, H_2, S_2, \ldots, S_m]/I_\Delta,$$

where $S_1, \ldots, S_m$ are the polynomials in A_Δ that correspond to the generators of the module of syzygies of the ideal $\langle \ell_1^{r+1}, \ldots, \ell_m^{r+1} \rangle$ in R generated by the linear forms ℓ_i corresponding to the interior edges of Δ.

Following these ideas, a similar construction leads to a conjecture for $C^r(\Delta)$ of a generic triangulation Δ, where G_Δ a connected graph with a finite number of cycles [7].

There are still many open problems concerning spline spaces, and knowing about their algebraic structure might bring some light and useful results for computation. As a consequence of the relation of $C^0(\Delta)$ with A_Δ, the dimensions as vector spaces over $\mathbb{R}$ of the subspaces $C_k^0(\Delta)$ were derived [2]. Similarly, the Proposition 2.2 and Conjecture 2.3 may lead to find the dimension of $C_k^r(\Delta)$ for splines of higher order of smoothness.

References

[1] L. J. Billera, *Homology of smooth splines: generic triangulations and a conjecture of Strang*, Trans. Amer. Math. Soc. **310** (1988), no. 1, 325–340.

[2] ———, *The algebra of continuous piecewise polynomials*, Adv. Math. **76** (1989), no. 2, 170–183.

[3] L. J. Billera and L. L. Rose, *A dimension series for multivariate splines*, Discrete Comput. Geom. **6** (1991), no. 2, 107–128.

[4] B. Mourrain and N. Villamizar, *Homological techniques for the analysis of the dimension of triangular spline spaces*, J. Symbolic Comput. **50** (2013), 564–577.

[5] ———, *Bounds on the dimension of trivariate spline spaces: a homological approach*, to appear in Mathematics in Computer Sciences, special issue on computational algebraic geometry (2014).

[6] H. Schenck, *Subalgebras of the Stanley-Reisner ring*, Discrete Comput. Geom. **21** (1999), no. 4, 551–556.

[7] N. Villamizar, *Algebraic Geometry for Splines*, Doctoral dissertation, University of Oslo http://urn.nb.no/URN:NBN:no-38634 (2012).

RICAM, Austrian academy of sciences. Altenberger strasse 69, 4040 Linz, Austria.
E-mail address: nelly.villamizar@oeaw.ac.at

NONLINEAR q-ARY CODES: CONSTRUCTIONS AND MINIMUM DISTANCE COMPUTATION

MERCÈ VILLANUEVA, FANXUAN ZENG, AND JAUME PUJOL

ABSTRACT. A nonlinear code can be represented as the union of cosets of a linear subcode. Properties and constructions of new codes from given ones in terms of this representation can be described. Algorithms to compute the minimum distance of nonlinear codes, based on known algorithms for linear codes, are also established. Moreover, the performance of these algorithms is studied and an estimation of the number of enumerated codewords needed in the computations is given.

INTRODUCTION

Let $\mathbb{F}_q$ be a finite field with q elements and let $\mathbb{F}_q^n$ be the set of all vectors of length n over $\mathbb{F}_q$. The *Hamming distance* $d(u, v)$ between $u, v \in \mathbb{F}_q^n$ is the number of coordinates in which u and v differ. The *Hamming weight* $wt(u)$ of $u \in \mathbb{F}_q^n$ is $wt(u) = d(u, \mathbf{0})$, where $\mathbf{0}$ is the all-zero vector of length n. An (n, M, d) *q-ary code* C is a subset of $\mathbb{F}_q^n$ with M codewords and minimum distance d. The vectors of a code are called *codewords* and the *minimum distance*, denoted by $d(C)$, is the minimum value of $d(u, v)$ for all $u, v \in C$ and $u \neq v$.

Two q-ary codes C_1 and C_2 of length n are said to be *equivalent* if there is a vector $a \in \mathbb{F}_q^n$, a monomial matrix $\mathcal{M}$ and an automorphism Γ of the field $\mathbb{F}_q$ such that $C_2 = \{\mathcal{M}\Gamma(c)+a \, : \, c \in C_1\}$. Note that two equivalent codes have the same minimum distance. If C is linear, then $\mathbf{0} \in C$; but if C is nonlinear, then $\mathbf{0}$ does not need to belong to C. In this case, we can always consider a new code $C' = C - c$ for any $c \in C$, which is equivalent to C, such that $\mathbf{0} \in C'$. Therefore, from now on, we assume that $\mathbf{0} \in C$.

Given a q-ary code C, the problem of storing C in memory is a well known problem. If C is linear, that is, it is a subgroup of $\mathbb{F}_q^n$, then it can be compactly represented using a generator matrix. On the other hand, if C is nonlinear, it can be seen as the union of cosets of a linear subcode of C [7]. This allows us to represent a code as a set of representative codewords instead of as a set with all codewords.

Computing the minimum distance of a q-ary code C is necessary in order to establish its error-correcting capability. However, this problem is computationally difficult, and has been proven to be NP-hard [4]. If C is linear, $d(C)$ coincides with the minimum weight, denoted by $wt(C)$, and the Brouwer-Zimmermann minimum weight algorithm for linear codes over finite fields [1, 6] can be used. This algorithm can be found implemented in the computational algebra system MAGMA [2, 3, 5]. On the other hand, if C is nonlinear, $wt(C)$ and $d(C)$ do not always coincide, and as far as we know there is not any algorithm to compute them comparable to Brouwer-Zimmermann algorithm for linear codes.

This work has been partially supported by the Spanish MICINN under Grants TIN2010-17358 and TIN2013-40524-P, and by the Catalan AGAUR under Grant 2009SGR1224.

1. Representation and Construction of Nonlinear Codes

The *kernel* of a q-ary code C is defined as $K_C = \{x \in \mathbb{F}_q^n : \lambda x + C = C \ \forall \lambda \in \mathbb{F}_q\}$ [7]. Since $\mathbf{0} \in C$, K_C is a linear subcode of C. We denote by κ the dimension of K_C. In general, C can be written as the union of cosets of K_C, and K_C is the largest such linear code for which this is true [7]. Therefore, $C = \bigcup_{i=0}^{t}(K_C + v_i)$, where $v_0 = \mathbf{0}$, $t+1 = M/q^\kappa$, $M = |C|$ and $L = \{v_1, \dots, v_t\}$ is the set of coset leaders. Note that for binary codes, $t \neq 1$, because if $t = 1$, $C = K_C \cup (K_C + v_1)$, but then C would be linear, so $C = K_C$. It is also important to emphasize that the coset leaders in this paper are not necessarily the ones having minimum weight in each coset. Since K_C is linear, it can be compactly represented by its generator matrix G of size $\kappa \times n$. Then, since the kernel takes up a memory space of order $O(n\kappa)$, the kernel plus the t coset leaders take up a memory space of order $O(n(\kappa + t))$.

Using this representation, we can manipulate and construct new nonlinear codes from old ones in a more efficient way. Specifically, it is possible to show how to establish the equality and inclusion of two given nonlinear codes from their kernels and coset leaders, and how to compute the kernel and coset leaders of new codes (union, intersection, extended, punctured, shorten, direct sum, Plotkin sum) from given ones, which are already represented in this way. All these results can be written to be implemented easily as algorithms. We can obtain the kernel and coset leaders of an extended code directly from the kernel and coset leaders of the code. The same happens for the direct sum and Plotkin sum constructions. For all other constructions, we obtain a partial kernel and the corresponding coset leaders. Although we can not assure which are the final kernel and coset leaders in these cases, we can speed up the kernel computation by starting from a partial kernel.

2. Minimum Distance Computation

The best known enumerative algorithm for linear codes to compute the minimum weight is the Brouwer-Zimmermann algorithm, which is based on the next result [5]. Let G be a generator matrix of a linear code K of dimension κ over $\mathbb{F}_q$. Any set of κ coordinates such that the corresponding columns of G are linear independent is called an *information set* for K. Let $G_1, \dots, G_h$ be h systematic generator matrices of K such that they have pairwise disjoint information sets. For any $r < \kappa$, if $S_i = \{mG_i : m \in \mathbb{F}_q^k,\ wt(m) \leq r\}$ for each matrix G_i, then all $c \in C \backslash \bigcup_{i=1}^{h} S_i$ satisfy $wt(c) \geq h(r+1)$. After the rth step, we obtain a lower bound $h(r+1)$ and an upper bound of the minimum weight, which is the minimum weight of the enumerated codewords. When the two bounds meet, we obtain $wt(K)$ without enumerating necessarily all codewords. An adaption of this algorithm enables the use of more generator matrices with overlapping information sets, which means that the lower bound can grow faster during the enumeration process.

Given a q-ary linear code K of dimension κ and a vector $v \in \mathbb{F}_q^n \backslash K$, the linear span $K_v = \langle K, v \rangle = \bigcup_{\lambda \in \mathbb{F}_q}(K + \lambda v)$ of dimension $\kappa + 1$ is called an *extend coset.*

Proposition 2.1. *Let* $C = \bigcup_{i=0}^{t}\left(K_C + v_i\right)$. *The minimum distance* $d(C)$ *can be computed as* $\min(\{wt(K_{v_j - v_i}) \ : \ i \in \{0, 1, \dots, t-1\},\ j \in \{i+1, \dots, t\}\})$, *where* $v_0 = \mathbf{0}$.

Using the representation of nonlinear codes given in Section 1, Proposition 2.1 and the Brouwer-Zimmermann algorithm, we can design a new algorithm (MinD) to compute the minimum distance of a nonlinear code C, based on computing $wt(K_{v_j - v_i})$ using the known Brouwer-Zimmermann algorithm. Note that the complexity of this algorithm depends strongly on the number of coset

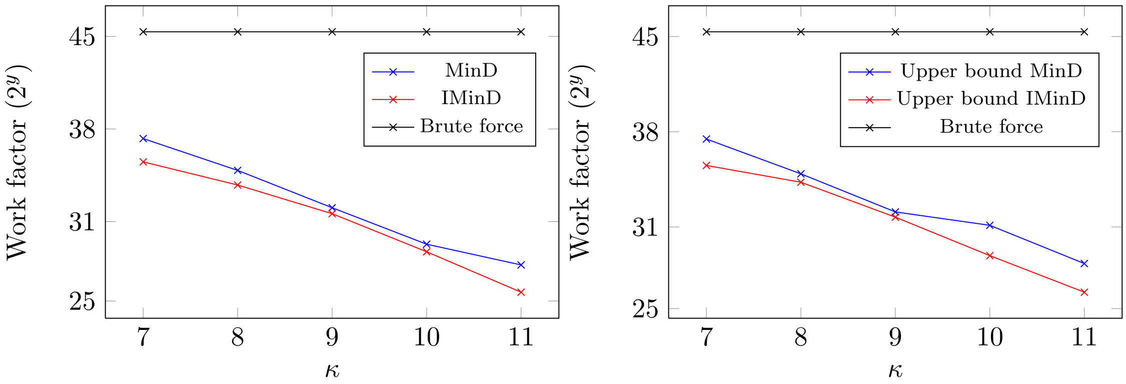


FIGURE 1. Work factors and upper bounds for computing $d(C)$ of ternary nonlinear codes C of length $n = 100$ and size $M = 3^{11} \cdot 6$.

leaders t and the complexity of the Brouwer-Zimmermann algorithm, since we need to compute $\binom{t+1}{2}$ times the minimum weight of a linear code.

This Algorithm MinD is based on the enumeration of codewords, adding together codewords and determining their minimum weight. The nature of these computations gives rise to a natural performance measure, which is referred to as *work* [5]. One unit of work represents both an addition and the weight computation of a single coordinate position. An estimate of the total work an algorithm performs is referred to as *work factor*. Therefore, work factors provide us with a tool for comparing the performance of algorithms based on enumeration. For example, note that the work factor for computing the minimum distance using a brute force algorithm is $\log_2(q)n\binom{q^\kappa(t+1)}{2}$.

Proposition 2.2. *Let C be a nonlinear code of length n with kernel of dimension κ and coset leaders $\{v_1, \ldots, v_t\}$. The work factor for computing $d(C)$ using Algorithm MinD is*

$$(1) \qquad \sum_{i=0}^{t-1}\Big(\sum_{j=i+1}^{t}\Big(\log_2(q)(n-\kappa-1)\lceil n/(\kappa+1)\rceil\sum_{r=1}^{\bar{r}_{i,j}}\binom{\kappa+1}{r}(q-1)^{r-1}\Big)\Big)$$

where $\bar{r}_{i,j}$ is the smallest integer such that $\lfloor n/(\kappa+1)\rfloor(\bar{r}_{i,j}+1) + \max(0, \bar{r}_{i,j}+1-(\kappa+1-n \mod (\kappa+1))) \geq wt(K_{v_j-v_i})$.

Note that the work factor for computing $d(C)$ relies on the parameters $\bar{r}_{i,j}$, which depend on $wt(K_{v_j-v_i})$, and they may be different for any i, j. Therefore, it is impossible to estimate the work factor if only the values n, κ and t are given. However, we can consider an upper bound of the work factor, and from that be able to estimate easily the work factor for computing $d(C)$. Since for any extend coset K_v we have that $wt(K_v) \leq wt(K_C)$, we can obtain an upper bound by replacing $wt(K_v)$ with $wt(K_C)$.

Proposition 2.3. *Let C be a nonlinear code of length n with kernel K_C of dimension κ and t coset leaders. An upper bound for the work factor of computing $d(C)$ using Algorithm MinD is given by*

$$(2) \qquad \binom{t+1}{2}\log_2(q)(n-\kappa-1)\lceil n/(\kappa+1)\rceil\sum_{r=1}^{\bar{r}}\binom{\kappa+1}{r}(q-1)^{r-1}$$

where $\bar{r}$ is the smallest integer such that $\lfloor n/(\kappa+1)\rfloor(\bar{r}+1)+\max(0,\bar{r}+1-(\kappa+1-n \mod (\kappa+1))) \geq wt(K_C)$.

From Algorithm MinD, it is easy to see that the weight of some codewords in the kernel K_C is computed several times, specifically, once for each $K_{v_j-v_i}$, where $i,j \in \{0,1,\ldots,t\}$ and $i<j$. Moreover, we need to compute the weight of extra vectors which belong to $K_C+\lambda(v_j-v_i)$, where $\lambda \in \mathbb{F}_q\backslash\{0,1\}$. However, we can make a little adjustment to the algorithm, in order to avoid this extra computation. In Brouwer-Zimmermann algorithm, the enumerating process is divided into several steps. In the rth step, it enumerates all linear combinations of r rows of the generator matrix of $K_{v_j-v_i}$ of dimension $\kappa+1$, examines the minimum weight of each combination and compares it with the lower bound. We can simplify this and enumerate only the codewords in each coset $K_C+v_j-v_i$. Then, in the rth step, we enumerate all linear combinations of r rows of the generator matrix of K_C of dimension κ and compute the weight of each combination adding the vector v_j-v_i. After this adjustment, the work factor using the improved Algorithm MinD, which is referred as Algorithm IMinD, can be reduced. Moreover, as before, we can also establish an upper bound for the work factor by using the same argument as in Proposition 2.3. Using this upper bound, again it is possible to estimate the work factor for computing $d(C)$ from the parameters n, κ, t and $wt(K_C)$ of a q-ary nonlinear code C. Note that the results on these upper bounds for the work factors allow to establish from which parameters of the given code, it is better to use the new presented algorithms instead of the brute force method.

Figure 1 shows the work factors (and the work factors upper bounds) for computing $d(C)$ using Algorithms MinD, IMinD and brute force, respectively. Note that when κ is large, Algorithms MinD and IMinD save a lot of time. Moreover, we can see the improvement on Algorithm MinD. In both tables, the work factors are expressed in logarithmic scale.

REFERENCES

[1] A. Betten, H. Fripertinger, A. Kerber, A. Wassermann, and K.-H. Zimmermann, *Codierungstheorie: Konstruktionen und Anwendung linearer Codes*, Berlin: Springer, 1998.

[2] J. J. Cannon and W. Bosma (Eds.), *Handbook of* MAGMA *Functions*, Edition 2.13, 4350 pages, 2006.

[3] M. Grassl, "Searching for linear codes with large minimum distance," in: W. Bosma and J. Cannon (Eds.) *Discovering Mathematics with Magma*, Springer, 2006.

[4] A. Vardy, "The intractability of computing the minimum distance of a code," *IEEE Trans. Inform. Theory*, vol. 43, no. 6, pp. 1757-1773, 1997.

[5] G. White, *Enumeration-based Algorithms in Coding Theory*, PhD Thesis, University of Sydney, 2006.

[6] K.-H. Zimmermann, "Integral Hecke Modules, Integral Generalized Reed-Muller Codes, and Linear Codes," Tech. Rep. 3-96, Technische Universität Hamburg-Harburg, 1996.

[7] K. T. Phelps, J. Rifà, M. Villanueva, "Kernels and p-kernels of p^r-ary 1-perfect codes," *Designs, Codes and Cryptography*, 37, 243-261, 2001.

Universitat Autònoma de Barcelona
E-mail address: merce.villanueva@uab.cat, fanxuan@deic.uab.cat, jaume.pujol@uab.cat

List of participants

Marta Abril Bucero Inria Sophia Antipolis
Maria Alberich-Carramiñana Universitat Politècnica de Catalunya
María Emilia Alonso Universidad Complutense de Madrid
Josep Alvarez Montaner Universitat Politècnica de Catalunya
Mauro C. Beltrametti Università de Genova
Christian Berghoff University of Bonn
Isabel Bermejo Universidad de La Laguna
Cristina Bertone Università di Torino
Mohamed Salah Boudellioua Sultan Qaboos University
Marta Casanellas Rius Universitat Politècnica de Catalunya
Manuel Ceballos Universidad de Sevilla
Iuliana Ciocanea Teodorescu Leiden University
Mihai Cipu Simion Stoilow Institute of Mathematics of the Romanian Academy Bucharest
Laura Colmenarejo Universidad de Sevilla
Gemma Colomé Nin Universitat Pompeu Fabra
Robert Corless Western University
Teresa Cortadellas Universitat de Barcelona
Ferran Dachs Cadefau Universitat Politècnica de Catalunya
Carlos D'Andrea Universitat de Barcelona
Gema María Díaz Toca Universidad de Murcia
Christian Eder University of Kaiserslautern
Joan Elias Universitat de Barcelona
Matthew England University of Bath
Ujué Etayo Rodríguez Universidad de Valladolid
Ahlam Fallatah Taibah University
Elisenda Feliu University of Copenhagen
Alberto Fernandez Boix Universitat Pompeu Fabra
Oscar Fernández Ramos Universita di Genova
Jesús Fernández Sánchez Universitat Politècnica de Catalunya
Mario Fioravanti Universidad de Cantabria
Matteo Gallet JKU - University of Linz
André Galligo University of Nice
Eva García Llorente Universidad de La Laguna
Ignacio García Marco Université Montpellier 2
Xabier García Martínez Universidad de Santiago de Compostela

Philippe Gimenez Universidad de Valladolid
José Gómez-Torrecillas Universidad de Granada
Maximilian Jaroschek Johannes Kepler University
Haydee Jiménez Tafur Universidad de Sevilla
Deepak Kapur University of New Mexico
Ekaterina Karatsuba Russian Academy of Sciences
Tetiana Klymchuk Taras ShevchenkoNational University of Kyiv
Manuel Ladra Universidad de Santiago de Compostela
Gadea Mata Universidad of La Rioja
Robert H C Moir Western University
Antonio Montes Universitat Politècnica de Catalunya
M. Eulàlia Montoro Universitat de Barcelona
Bernard Mourrain INRIA Sophia-Antipolis
Marta Narváez Clauss Universidad de Barcelona
Gabriel Navarro Universidad of Granada
Douglas Navarro Universidad Nacional
Tomas Recio Universidad of Cantabria
Aureliano M. Robles-Pérez Universidad of Granada
Ana Romero Universidad de La Rioja
Julio Rubio Universidad de La Rioja
Eduardo Sáenz de Cabezón Universidad de La Rioja
Francisco Santos Universidad of Cantabria
Adrian Segura Moreiras Universitat Pompeu Fabra
Juan Rafael Sendra Pons Universidad de Alcalá
Martin Sombra Universitat de Barcelona
Hayden Stainsby Universitat Autònoma de Barcelona
Klara Stokes Fundació per a la Universitat Oberta de Catalunya
Luis Felipe Tabera Alonso Universidad de Cantabria
Steven Thornton Western University
Maria-Laura Torrente Università de Genova
Nelly Villamizar Austrian Academy of Sciences
Martin Weimann Université de Caen
Giuseppe Zappala Università di Catania
Santiago Zarzuela Universitat de Barcelona
Fanxuan Zeng Universitat Autònoma de Barcelona