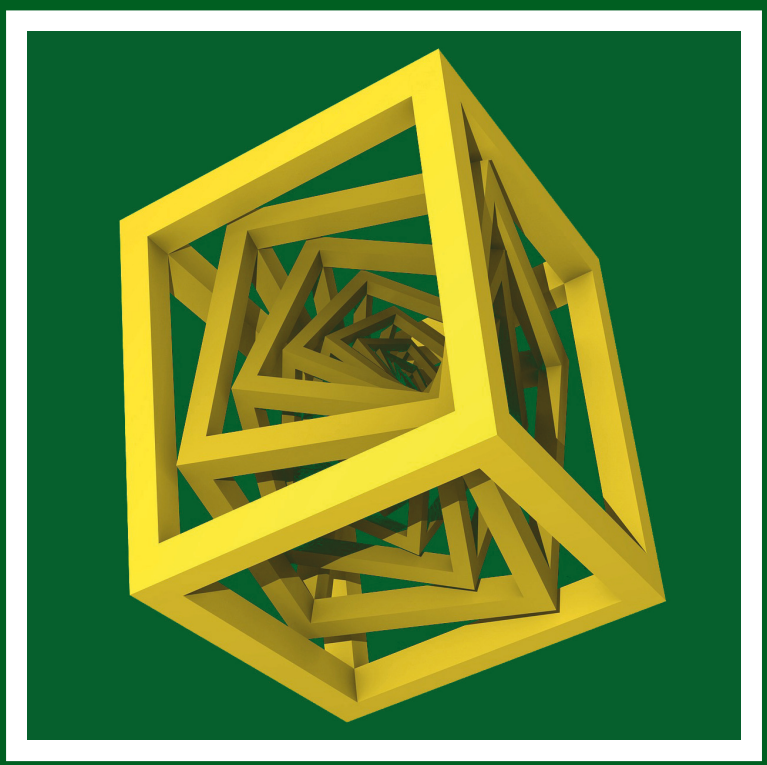
UNIVERSITAT JAUME I

EACA 2022

XVII Encuentro de Álgebra Computacional y Aplicaciones

XVII Meeting on Computer Algebra and Applications

Carlos Galindo, Philippe Giménez,
Fernando Hernando, Francisco J. Monserrat,
Julio José Moyano Fernández (coord.)



COL·LECCIÓ
TREBALLS D'INFORMÀTICA I TECNOLOGIA
NÚM. 51

Col·lecció
«Treballs d'Informàtica i Tecnologia»
Núm. 51

EACA 2022

XVII Encuentro de Álgebra Computacional y Aplicaciones

XVII Meeting on Computer Algebra and Applications

Carlos Galindo, Philippe Giménez, Fernando Hernando,
Francisco J. Monserrat, Julio José Moyano Fernández (coord.)

UJI UNIVERSITAT JAUME I

BIBLIOTECA DE LA UNIVERSITAT JAUME I. Datos catalográficos

Noms: EACA. (17é : 2022 : Castelló de la Plana), autor | Galindo Pastor, Carlos, editor literari | Gimenez, Philippe, editor literari | Hernando Carrillo, Fernando, editor literari | Monserrat Delpalillo, Francisco José, editor literari | Moyano-Fernández, Julio José, editor literari | Universitat Jaume I. Publicacions, entitat editora

Altres títols: XVII Encuentro de Álgebra Computacional y Aplicaciones | XVII Meeting on Computer Algebra and Applications

Títol: EACA 2022 : XVII Encuentro de Álgebra Computacional y Aplicaciones = XVII Meeting on Computer Algebra and Applications / Carlos Galindo, Philippe Giménez, Fernando Hernando, Francisco J. Monserrat, Julio José Moyano Fernández (coord.)

Descripció: Castelló de la Plana : Publicacions de la Universitat Jaume I. Servei de Comunicació i Publicacions, [2023] | Col·lecció: Treballs d'informàtica i tecnologia ; 51 | Inclou referències bibliogràfiques | Textos en anglès

Identificadors: 978-84-19647-46-7

Matèries: Àlgebra – Congressos

Classificació: CDU 512(063) | THEMA PBF

Edita: Publicacions de la Universitat Jaume I. Servei de Comunicació i Publicacions
Campus del Riu Sec. Edifici Rectorat i Serveis Centrals. 12071 Castelló de la Plana
http://www.tenda.uji.es e-mail: publicacions@uji.es

ISBN papel: 978-84-19647-46-7
DOI: http://dx.doi.org/10.6035/INFiTEC.51

Depósito legal: CS 708-2023

Publicacions de la Universitat Jaume I es miembro de la UNE, lo que garantiza la difusión y comercialización de sus publicaciones a nivel nacional e internacional. www.une.es.

CONTENTS

FOREWORD

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

Over the years these meetings have achieved greater international recognition, especially from members of the Symbolic Computation community. They started in Santander in 1995 and have been held annually in Sevilla, Granada, Sigüenza, Tenerife, Barcelona, and Ezcaray. Starting in 2002 in Valladolid, they have been held biannually in Santander, Sevilla, Granada, Santiago de Compostela, Alcalá de Henares, Barcelona, Logroño and Zaragoza (in July 2018). Although the seventeenth edition was scheduled to be held in Castelló de la Plana in 2020, it had to be postponed due to the COVID-19 pandemic ,until June 2022, the current edition.

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

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

The XVII Meeting on Computer Algebra and Applications (EACA 2022) will take place in Castelló de la Plana, at Universitat Jaume I, from June 20 to June 22. This activity of the EACA network is part of the «Redes de Investigación» Dynamisation Actions RED2018-102583-T, partially supported by the Spanish research ministry and agency MCIN/AEI/10.13039/501100011033/.

This book contains the extended abstracts of the accepted contributions and the plenary talks for this 17th edition of EACA. There are a total of 27 contributions, accepted after a standard referee process, and 5 plenary talks. The plenary speakers are:

- Rocío González Díaz, Universidad de Sevilla (Spain),
- Gregor Kemper, Technische Universität München (Germany),
- Pierre Lairez, INRIA Saclay Île-de-France (France),
- Sonia Pérez Díaz, Universidad de Alcalá (Spain), and
- Diego Ruano, Universidad de Valladolid (Spain).

We would like to express our sincere gratitude to the members of the Scientific Committee, chaired by Manuel Ladra (Universidad de Santiago de Compostela), María Emilia Alonso (Universidad Complutense de Madrid), Enrique Artal (Universidad de Zaragoza), Marta Casanellas (Universitat Politècnica de Catalunya), Francisco J. Castro (Universidad de Sevilla), Carlos D'Andrea (Universitat de Barcelona), Ignacio García Marco (Universidad de La Laguna), Philippe Gimenez (Universidad de Valladolid), José Gómez-Torrecillas (Universidad de Granada), Laureano González-Vega (Universidad de Cantabria), Jorge Martín Morales (Universidad de Zaragoza), Francisco J. Monserrat (Universitat Politècnica de València), Sonia Pérez (Universidad de Alcalá), and Ana Romero (Universidad de la Rioja). Our gratitude also goes to Universitat Jaume I, Instituto Universitario de Matemáticas y Aplicaciones de Castellón (IMAC), Escola Superior de Tecnologia i Ciències Experimentals de la Universitat Jaume I, Fundació Universitat Jaume I-Empresa (FUE) and to the following institutions that have offered us financial support:

- Ministerio de Ciencia e Innovación,
- Foundation Compositio Mathematica,
- Diputació de Castelló.

Finally, we would like to give special thanks to Helena Martín Cruz and Elvira Pérez Callejo for their dedication and collaboration in the organization of this event.

It has been a great pleasure for us to contribute to make this event possible. We wish all the participants in this meeting a successful and fruitful conference and a very pleasant and productive stay in Castelló de la Plana.

The organizing committee:

C. Galindo, P. Gimenez, F. Hernando
F. Monserrat , J. J. Moyano

Castelló de la Plana, June 2022

PLENARY TALKS

PARTIAL FUNCTIONS INDUCED BY MORPHISMS BETWEEN OF PERSISTENCE MODULES

R. GONZALEZ-DIAZ, M. SORIANO-TRIGUEROS, AND A. TORRAS-CASAS

ABSTRACT. Persistence modules are fundamental algebraic structures in topological data analysis. One often needs to understand morphisms between a pair of persistence modules as these appear very naturally in practical situations. Even though one might express such morphisms as the direct sum of indecomposable modules, in most cases the decomposition is out of our reach. We define an easy-to-compute partial function relating the interval decomposition of the domain and codomain of such morphisms. This approach gives information about the inner structure of the morphism in a computable way, allowing their use in topological data analysis.

1. BACKGROUND ON PERSISTENCE MODULES

A *persistence module* V is a functor from $\mathbb{R}$ to Vect, the category of vector spaces over a field k with unit denoted by 1_k. In other words, V is a set of vector spaces V_t for all $t \in \mathbb{R}$ and a set of linear maps $\rho_{st} : V_s \to V_t$ for all pairs $s \leq t$, such that $\rho_{st} \circ \rho_{rs} = \rho_{rt}$ if $r \leq s \leq t$ and $\rho_{tt} = \mathrm{Id}_{V_t}$ for all $t \in \mathbb{R}$; where Id_{V_t} denotes the identity map. The linear maps ρ_{st} will be called the *structure maps* of V.

A *morphism between persistence modules*, $f : V \to U$, is a natural transformation between them. It consists of a set of linear functions $\{f_t : V_t \to U_t\}$ which commutes with respect to the structure maps.

We will use enriched numbers, $\mathbb{E} = \mathbb{R} \times \{+, -\} \cup \{-\infty, \infty\}$, to represent intervals:

$(\cdot, \cdot)$	q^-	q^+	∞
$-\infty$	$(-\infty, q)$	$(-\infty, q]$	$(-\infty, \infty)$
p^-	$[p, q)$	$[p, q]$	$[p, \infty)$
p^+	(p, q)	$(p, q]$	(p, ∞)

Example 1.1. Given an interval $(a, b) \subset \mathbb{R}$, let us consider a persistent module $k_{(a,b)}$ given by

$$k_{(a,b)t} = \begin{cases} k & \text{if } t \in (a, b), \\ 0 & \text{otherwise,} \end{cases}$$

with $\rho_{st} = \mathrm{Id}_k$ for all $s, t \in (a, b)$ with $s \leq t$. We call $k_{(a,b)}$ an *interval module*.

Example 1.2. Given two interval modules $k_{(a,b)}$ and $k_{(c,d)}$ with $c \leq a \leq d \leq b$, we define a morphism $f : k_{(a,b)} \to k_{(c,d)}$ as

$$f_t = \begin{cases} \mathrm{Id}_k & \text{if } t \in (a, d), \\ 0 & \text{otherwise.} \end{cases}$$

The authors have been partially supported by the Agencia Estatal de Investigación/10.13039/501100011033 grant PID2019-107339GB-100 and the Agencia Andaluza del Conocimiento grant P20-01145.

The talk at the EACA 2022 meeting was given by the first author.

Contents

Note that in Example 1.2, all inequalities $c \leq a \leq d \leq b$ must hold, since otherwise f cannot commute with the structure maps from $k_{(a,b)}$ and $k_{(c,d)}$. The next theorem justifies the use of interval modules as the building blocks of persistence modules.

Theorem 1.3. [1] *Let V be a persistence module. Suppose that V satisfies some mild assumptions. Then V decomposes uniquely, up to isomorphisms, as:*

$$V \simeq \bigoplus_{I \in S} m_I k_I$$

where S is a set of intervals and m_I their multiplicity.

By Theorem 1.3, a persistent module V is completely determined up to isomorphism by the set $bar(V) = \{(I, m_I)\}_{I \in S}$. From $bar(V)$ we may define the ordered set $\{(a_i, b_i)\}_{i=1}^{N}$ where each interval I appears as many times as its multiplicity m_I.

A *barcode basis* $\mathcal{A}$ for V is a choice of an isomorphism:

$$\alpha : \bigoplus_{i=1}^{N} k_{(a_i,b_i)} \to V.$$

We may restrict each summand of α to its domain interval module $\alpha_i : k_{(a_i,b_i)} \to \mathbb{V}$ for all $1 \leq i \leq N$. We will write $\alpha_i \sim (a_i, b_i)$ and denote a barcode basis by the set $\mathcal{A} = \{\alpha_i\}_{i=1}^{N}$.

Example 1.4. Let $V \simeq k_{(0^-,4^-)} \oplus k_{(1^+,3^+)}$ be a persistence module. We take the barcode basis given by $\alpha_1 \sim (0^-, 4^-)$ and $\alpha_2 \sim (1^+, 3^+)$, and depict the interval decomposition as:

Unfortunately, the decomposition of morphisms between persistence modules is much more complex than that of persistence modules. In particular, the set of possible indecomposables is known to be wild in the general case [2]. We are interested in computable tools to distinguish between such morphisms.

2. The Induced partial function

In this section, given $f : V \to U$, we propose a partial function, $\mathcal{M}_f$, relating $bar(V)$ with $bar(U)$. Differences between $\mathcal{M}_f$ and $\mathcal{M}_g$ will outline differences between the original morphisms f and g.

Given $I \in bar(V)$ and $J \in bar(U)$, $\mathcal{M}_f$ returns $\mathcal{M}_f(I, J) \in \mathbb{N} \cup \{0\}$ such that

$$\sum_J \mathcal{M}_f(I, J) \leq m_I.$$

One may interpret $\mathcal{M}_f$ as a *partial function* that sends intervals in $bar(V)$ to intervals in $bar(U)$.

Given a subset of a base $\mathcal{S} \subseteq \mathcal{A} = \{\alpha_i\}_{i=1}^{N}$ for V, we define $\langle \mathcal{S} \rangle$ as the submodule of V given by the image of $\alpha : \bigoplus_{\alpha_i \in \mathcal{S}} k_{(a_i,b_i)} \to V$. We will denote by $\mathcal{S}_t$ the base for $\langle \mathcal{S} \rangle_t$ for all $t \in \mathbb{R}$, which corresponds to the set

$$\left\{ \alpha_{it}(1_k) \mid \alpha_i \in \mathcal{S} \text{ with } \alpha_i \sim (a_i, b_i) \text{ such that } t \in (a_i, b_i) \right\}.$$

Note that a barcode base leads to a pointwise base, that is, $\langle \mathcal{A}_t \rangle = \langle \mathcal{A} \rangle_t$ for all $t \in \mathbb{R}$.

Let $c \in \mathbb{E}$ and let $t \in (c, \infty)$. We consider the following operators over V:

$$\mathrm{Im}^+_{ct}(V) := \bigcap_{s\in(c,t^+)} \mathrm{Im}(\rho_{st}), \qquad \mathrm{Im}^-_{ct}(V) := \bigcup_{s\in(-\infty,c)} \mathrm{Im}(\rho_{st}), \qquad \text{for } t \in (c,\infty);$$

$$\mathrm{Ker}^+_{ct}(V) := \bigcap_{s\in(c,\infty)} \mathrm{Ker}(\rho_{st}), \qquad \mathrm{Ker}^-_{ct}(V) := \bigcup_{s\in(t^-,c)} \mathrm{Ker}(\rho_{st}), \qquad \text{for } t \in (-\infty,c).$$

Even though these operators do not depend on a base, they can be expressed using a fixed one. In order to achieve this, we need the following subsets of a base $\mathcal{A}$ for V:

- $\mathcal{I}^{\pm}_a = \left\{\alpha_i \in \mathcal{A} \mid \alpha_i \sim (a_i, b_i) \text{ such that } a_i \le a \text{ for } \mathcal{I}^+_a \text{ or } a_i < a \text{ for } \mathcal{I}^-_a\right\}$,
- $\mathcal{K}^{\pm}_b = \left\{\alpha_i \in \mathcal{A} \mid \alpha_i \sim (a_i, b_i) \text{ such that } b_i \le b \text{ for } \mathcal{K}^+_b \text{ or } b_i < b \text{ for } \mathcal{K}^-_b\right\}$.

Lemma 2.1. $\mathrm{Im}^{\pm}_{at}(V) = \langle \mathcal{I}^{\pm}_{at} \rangle$ *and* $\mathrm{Ker}^{\pm}_{bt}(V) = \langle \mathcal{K}^{\pm}_{bt} \rangle$ *for all* $t \in (a, b)$.

Given $t \in (a, b)$, let us define the following subspaces of $V(t)$:

$$V^+_{(a,b)t} = \mathrm{Im}^+_{at} \cap \mathrm{Ker}^+_{bt} \qquad \text{and} \qquad V^-_{(a,b)t} = \mathrm{Im}^-_{at} \cap \mathrm{Ker}^+_{bt} + \mathrm{Im}^+_{at} \cap \mathrm{Ker}^-_{bt}\,.$$

Now, let $\mathcal{A}^+_{(a,b)} = \mathcal{I}^+_a \cap \mathcal{K}^+_b$ and $\mathcal{A}^-_{(a,b)} = (\mathcal{I}^+_a \cap \mathcal{K}^-_b) \cup (\mathcal{I}^-_a \cap \mathcal{K}^+_b)$. We obtain the following result.

Proposition 2.2. $V^+_{(a,b)t} = \langle \mathcal{A}^+_{(a,b)t} \rangle$ *and* $V^-_{(a,b)t} = \langle \mathcal{A}^-_{(a,b)t} \rangle$ *for all* $t \in (a, b)$.

The spaces $V^{\pm}_*$ can be used to find the decomposition of V: see [1]. Next, we link $V^{\pm}_*$ with $U^{\pm}_*$ to define $\mathcal{M}_f$. Consider $(a, b) \in bar(V)$ and $(c, d) \in bar(U)$. Given $t \in (a, b) \cap (c, d)$, let us define $X_{(a,b)\,(c,d)t}$ and $\mathcal{M}_f$ as:

$$X_{(a,b)\,(c,d)t} := \frac{f_t\left(V^+_{(a,b)t}\right) \cap U^+_{(c,d)t}}{f_t\left(V^-_{(a,b)t}\right) \cap U^+_{(c,d)t} + f_t\left(V^+_{(a,b)t}\right) \cap U^-_{(c,d)t}},$$

$$\mathcal{M}_f((a, b), (c, d)) = \dim\left(\varinjlim_{t\in(a,b)\cap(c,d)} X_{(a,b)\,(c,d)t}\right).$$

Theorem 2.3. [3] $\mathcal{M}_f$ *is well-defined and linear:*

$$\mathcal{M}_{f^1\oplus f^2}((a, b), (c, d)) = \mathcal{M}_{f^1}((a, b), (c, d)) + \mathcal{M}_{f^2}((a, b), (c, d)).$$

3. Matrix Algorithm

In this section we will calculate $\mathcal{M}_f$ from a pair of bases $\mathcal{A}$ and $\mathcal{B}$ for V and U respectively. We will use the interval notation $I = (a, b)$ and $J = (c, d)$. Let $t \in \mathbb{R}$, and consider the inclusion $\imath_{It} : V^+_{It} \to V_t$ and the projection $\pi_{Jt} : U_t \to U_t/U^-_{Jt}$. We will use the matrix form of the composition $\pi_{Jt} \circ f_t \circ \imath_{It}$ on the bases $\mathcal{A}^+_{It}$ and $\mathcal{B}_t \setminus \mathcal{B}^-_{Jt}$:

$$\mathcal{L}_{IJt} := \left(\begin{array}{c|cc} & \mathcal{A}^-_{It} & \mathcal{A}^+_{It} \setminus \mathcal{A}^-_{It} \\ \hline \mathcal{B}^+_{Jt} \setminus \mathcal{B}^-_{Jt} & \text{Block 1} & \text{Block 2} \\ \mathcal{B}_t \setminus \mathcal{B}^+_J & * & * \end{array}\right)$$

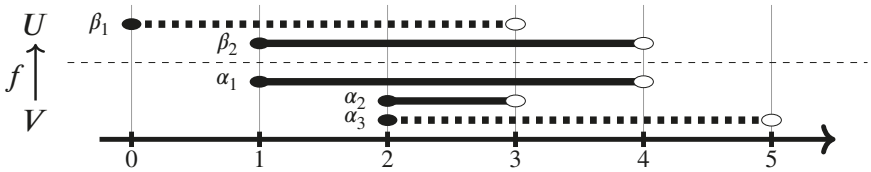
Consider the reduced matrix $\mathcal{N}_{IJt}$ obtained after a Gaussian elimination of $\mathcal{L}_{IJt}$ by using left to right column additions. For our calculation, we define some submatrices of $\mathcal{N}_{IJt}$ as follows. First,

ignore columns which are not zero on all rows in $\mathcal{B}_t \setminus \mathcal{B}_J^+$. Then, select the submatrices with rows in $\mathcal{B}_{Jt}^+ \setminus \mathcal{B}_{Jt}^-$ and columns in either $\mathcal{A}_{It}^+$, $\mathcal{A}_{It}^-$ or $\mathcal{A}_{It}^+ \setminus \mathcal{A}_{It}^-$. We name the resulting matrices as $\mathcal{R}_{IJt}^+$, $\mathcal{R}_{IJt}^-$ and $\mathcal{R}_{IJt}$. Note that $\mathcal{R}_{IJt}^-$ is contained within Block 1, $\mathcal{R}_{IJt}^f$ within Block 2 and $\mathcal{R}_{IJt}^+$ within both. The following result relates these submatrices with X_{IJt}, see [3, Theorem 5.5].

Theorem 3.1. *$X_{IJt} \simeq \langle \mathcal{R}_{IJt}^+ \rangle / \langle \mathcal{R}_{IJt}^- \rangle \simeq \langle \mathcal{R}_{IJt} \rangle$ for all $t \in I \cap J$.*

Here, $\langle R \rangle$ denotes the linear span of the set of the columns of R. We could then take the colimit of $\langle \mathcal{R}_{IJt} \rangle$ to obtain $\mathcal{M}_f(I, J)$. In practice, the colimit will be given by evaluating $\langle \mathcal{R}_{IJd} \rangle$ (that is, evaluating $\mathcal{R}_{IJt}$ in a value $t < d$ close enough to d) and $\mathcal{M}_f(I, J)$ is obtained by counting pivots.

Example 3.2. Let $J_1 = (0^-, 3^-), J_2 = (1^-, 4^-)$ as well as $I_1 = (1^-, 5^-)$, $I_2 = (2^-, 4^-)$ and $I_3 = (2^-, 5^-)$. We also consider $V \simeq k_{I_1} \oplus k_{I_2} \oplus k_{I_3}$ and $U \simeq k_{J_1} \oplus k_{J_2}$. We take the canonical bases $\mathcal{A} = \{\alpha_1, \alpha_2, \alpha_3\}$ for V and $\mathcal{B} = \{\beta_1, \beta_2\}$ for U (see below).



Next, we consider a morphism $f : V \to U$ which is determined (due to commutativity) by:

$$\alpha_1^1 \mapsto \beta_1^1 + \beta_2^1, \qquad \text{and} \qquad \alpha_2^2 \mapsto \beta_1^2 + \beta_2^2, \qquad \text{and} \qquad \alpha_3^2 \mapsto 2\beta_1^2 + \beta_2^2 \,.$$

Note that we have used the notation $\gamma_i^t = \gamma_{it}(1_k)$ for $t \in \mathbb{R}$ and $\gamma = \alpha, \beta$ and $1 \leq i \leq 3$. We obtain the matrices $\mathcal{L}_{I_i J_j *}$ for all $1 \leq i \leq 3$ and all $1 \leq ij \leq 2$, which we reduce if necessary:

$$\mathcal{L}_{I_1 J_1 3^-} = \mathcal{L}_{I_2 J_1 3^-} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad \mathcal{L}_{I_3 J_1 3^-} = \begin{pmatrix} 1 & 1 & 2 \\ 1 & 1 & 1 \end{pmatrix} \mapsto \mathcal{N}_{I_3 J_1 3^-} = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix},$$

$$\mathcal{L}_{I_3 J_2 4^-} = \mathcal{L}_{I_2 J_2 4^-} \begin{pmatrix} 1 \end{pmatrix}, \quad \mathcal{L}_{I_3 J_2 4^-} = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix} \mapsto \mathcal{N}_{I_3 J_2 4^-} = \begin{pmatrix} 1 & 0 & 0 \end{pmatrix}.$$

Altogether, we obtain:

$$\mathcal{R}_{I_1 J_1 3^-} = \mathcal{R}_{I_2 J_1 3^-} = \emptyset, \qquad \mathcal{R}_{I_3 J_1 3^-} = \begin{pmatrix} 1 \end{pmatrix}, \text{ and also}$$
$$\mathcal{R}_{I_1 J_2 4^-} = \mathcal{R}_{I_2 J_2 4^-} = \begin{pmatrix} 1 \end{pmatrix}, \quad \mathcal{R}_{I_3 J_2 4^-} = \emptyset.$$

Hence, $\mathcal{M}_f$ is interpreted as $I_1 \mapsto J_2$, $I_2 \mapsto J_2$ and $I_3 \mapsto J_1$.

References

[1] W. Crawley-Boevey, Decomposition of pointwise finite-dimensional persistence modules, Journal of Algebra and Its Applications 14 (5) (2015).

[2] E. Escolar, Y. Hiraoka, Persistence modules on commutative ladders of finite type, Discrete and Computational Geometry 55 (2014) 100–157.

[3] R. Gonzalez-Diaz, M. Soriano-Trigueros, A. Torras-Casas, Partial functions induced by maps of Persistence Modules. arXiv:2107.04519.

Universidad de Sevilla
Email address: rogodi@us.es, msoriano4@us.es, atorras@us.es

DISTANCE GEOMETRY, ALGEBRA AND DRONES

GREGOR KEMPER

Abstract. Is it always possible to reconstruct a point configuration in the plane from the unlabeled set of mutual distances between the points? This and other questions translate to invariant theory and ultimately into problems about polynomial ideals. As it turns out, the following question is related: can a drone detect the walls of a room from hearing the echoes of a sound? What if the time at which the sound was emitted is unknown? Attacking these questions again leads to ideal theory and requires massive computer algebra computations. The talk presents results by Mireille Boutin and the speaker, some of which are old and some very recent.

Technical University of Munich
Email address: kemper@ma.tum.de

Contents

MONODROMY IN COMPUTER ALGEBRA

PIERRE LAIREZ

Analytic continuation of a function of a complex variable along different paths with the same end points may lead to different values. This phenomenon is known as *monodromy*. I will show how to numerically compute the monodromy in several situations and focus on several applications building on the monodromy computation.

First, the computation of the irreducible decomposition of a complex algebraic curves, which will involve the monodromy of local parametrizations.

Second, the factorization of Fuchsian linear differential operators, which will involve the monodromy of a basis of solutions of a linear differential equation.

Lastly, we will consider the explicit computation of the homology of complex algebraic varieties, which will involve the monodromy of the homology groups of the fibers of a Lefschetz fibration.

Inria, France
Email address: pierre.lairez@inria.fr

Contents

ON THE PROBLEM OF POLYNOMIAL AND PROPER REPARAMETRIZATIONS OF ALGEBRAIC SURFACES

SONIA PÉREZ-DÍAZ

Abstract. In this talk, given a rational parametrization of an algebraic surface, we consider two different but related problems. First, we deal with the polynomial reparametrization problem. More precisely, we present an algorithm for reparametrizing birational surface parametrizations into birational polynomial surface parametrizations without base points, if they exist. Second, we develop an algorithm for reparametrizing non-birational surface parametrizations into birational surface parametrizations without base points, if they exist.

For both problems, we need some properties concerning base points. In particular, we show that the multiplicity of the base points locus of a projective rational surface parametrization can be expressed as the degree of the content of a univariate resultant. We use the degree formula relating the degree of the surface, the degree of the parametrization, the base points multiplicity, and the degree of the rational map induced by the parametrization. We extend both formulas to the case of dominant rational maps of the projective plane, and describe how the base point loci of a parametrization and its reparametrizations are related.

Once these results are introduced, in order to solve the problems considered, we impose a transversality condition on the base points of the input parametrization. Essentially, the idea of transversality is to assume that the multiplicity of the base points is minimal. Since this multiplicity is introduced as a multiplicity of intersection of two algebraic curves, it requires the transversality of the corresponding tangents.

Some crucial difficulties in many applications, and algorithmic questions, dealing with surface parametrizations are the presence of base points, the existence of non-constant denominators of the parametrizations and the birationality of the input parametrization. In this talk, we show how to provide a polynomial and also a birational parametrization with empty base locus, if they exist. Hence we provide algorithms to avoid the complications mentioned above, if is possible. For this purpose, we introduce, and indeed impose, the notion of transversal base locus. Here we consider the non-transversal case and we leave it as an open problem. We believe that using the ideas pointed out by J. Schicho in [4], on blowing up the base locus, it might be possible to transform the given problem (via a finite sequence of Cremone transformations and projective transformations) into the case of transversality.

The results presented are based on papers [1], [2] and [3].

References

1. J. Caravantes, S. Pérez-Díaz, J. R. Sendra. *Constructing proper reparametrizations for rational surfaces.* Submitted. 2022.

Supported by the Ministerio de Ciencia, Innovación y Universidades - Agencia Estatal de Investigación/PID2020-113192GB-I00 (Mathematical Visualization: Foundations, Algorithms and Applications). The author belongs to the ResearchGroup SYNACS (Ref.CCEE2011/R34).

2. D. Cox, S. Pérez-Díaz, J. R. Sendra. *On the base point locus of surface parametrizations: formulas and consequences*. Accepted. Communications in Mathematics and Statistics. 2021.
3. S. Pérez-Díaz, J. R. Sendra. *Computing birational polynomial surface parametrizations without base points*. Mathematics. DOI: 10.3390/math8122224. Vol. 8, 2224. 2020.
4. L. Schicho, J. *Simplification of surface parametrizations*. ISSAC 2002: Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation. ACM Press New York. pp. 229–237. 2002.

Universidad de Alcalá. Dpto. de Física y Matemáticas. Alcalá de Henares, Spain
Email address: sonia.perez@uah.es

ALGEBRAIC CODING THEORY AND SOME OF ITS APPLICATIONS

DIEGO RUANO

Abstract. In this talk, we will see how computer algebra can be applied to coding theory and some of its applications: secret sharing, multi-party computation, post-quantum cryptography, stabilizer quantum codes and private information retrieval.

1. Coding theory

Motivation? Data transmitted through modern digital communication systems may be corrupted by noise, resulting in a mismatch between the symbols sent and the symbols received. This may happen in satellite or mobile phone communication, and in internet connections, but also when storing data on a computer.

What is it? Error-correcting codes guarantee reliable and fast transmission of information in these systems by adding extra symbols to the information sent. Say that A would like to transmit some information to B. A will then create a codeword consisting of the information itself plus some additional symbols (this is called encoding) and subsequently send it to B. Even if B receives a corrupted ("noisy") version of the codeword sent, the extra symbols added in the encoding will allow B to recreate the original codeword in the decoding process, at least with high probability.

Challenge? The challenge is to construct codes which apart from correcting many errors using as few extra symbols as possible, can also provide fast en- and decoding algorithms. Moreover, implementations over a small finite field are desirable for practical implementations [36].

Performance? A linear code has three parameters $[n, k, d]$, where k is the number of information symbols, n is the total number of symbols (i.e. there are $n - k$ redundant symbols) and d is the minimum distance of the code. The minimum distance d tells us how many symbols may be corrected, since one can correct up to $d/2$ symbols, and it is equal to the minimum number of non-zero coordinates of a non-zero codeword. Hence, for a fixed value n, the aim is to obtain a linear code with k and d as high as possible. Obtaining codes with good parameters is a no trivial task since, although linear codes are just a vector subpace over a finite field, the minimum distance is not invariant by linear transformations. Moreover, given a generic code, computing its minimum distance is a difficult problem (NP-hard).

Reed-Solomon codes? Reed-Solomon codes are widely used since they have optimal parameters and fast en- and decoding algorithms. However, the length should be smaller than the finite field size, i.e. one needs a large finite field for a large code.

The author has been partially supported by Grant RYC-2016-20208 funded by MCIN/AEI/10.13039/501100011033 and "ESF Investing in your future", and Grant PGC2018-096446-B-C21 funded by MCIN/AEI/10.13039/501100011033 and "ERDF A way of making Europe".

Contents

Relation to Mathematics? Ever since the appearance of the area of coding theory in the late 1940's, algebraic, geometric and combinatorial methods have proven paramount tools for dealing with and describing the problems arising in the construction and usage of error-correcting codes. As a side effect, many interesting and sometimes challenging mathematical problems arose in this field.

Relation to Algebra? Evaluation codes have achieved important milestones in coding theory and are widely used. This is the case of algebraic-geometry codes [31], which are obtained by evaluating rational functions with bounded poles and zeros at points on an algebraic curve, and affine variety codes [25], which are obtained by evaluating polynomials at the zeros of a system of equations given by an ideal in a ring of polynomials, such as Reed-Muller codes and J-Affine codes [22]. One of the peculiarities of these codes is that they permit an algebraic formulation, since the parameters of the code are directly related to the ideal associated with the evaluation application. This means these codes can be studied with computer algebra techniques, like Gröbner bases, which provides the code with much more structure and its parameters can be estimated. For example, the footprint of an ideal provides a lower bound for the minimum distance [26].

Why are they not used by industry? Despite the very useful features of algebraic-geometry codes and affine-variety codes they do not always meet the requirements of applications in the industry (in coding theory). However, they can be used for practical cryptographic applications, as secret sharing, multi-party computation, post-quantum cryptography, quantum stabilizer codes and private information retrieval.

2. Secret Sharing

What is it? A secret sharing scheme is a cryptographic method to encode a secret into multiple shares subsequently distributed to participants, so that only specified sets of participants can reconstruct the secret. Secret sharing schemes have been used to store confidential information to multiple locations geographically apart, and they have several applications in computer science (see [12] and its references), the main one is multi-party computation. This is a challenging branch of cryptography where the adversaries are not only external but may be some of the participants.

Construction? Any linear secret sharing scheme can be obtained using a pair of nested linear codes [10], this gives the advantage of using the rich theory of linear codes. The first secret sharing scheme was proposed by Shamir in 1979 and it can be understood as a scheme coming from a pair of Reed-Solomon codes [42]. We therefore have the following issue: if we have to consider a large number of participants, we should work over a large finite field, but a small finite field is desirable for a practical implementation.

More efficient schemes (but not perfect)? Shamir's secret sharing scheme is a perfect scheme, in which a set of participants unable to reconstruct the secret has absolutely no information on the secret. Later, non-perfect secret sharing schemes (or ramp schemes) were proposed [1] where there are sets of participants that have a non-zero amount of information about the secret but cannot reconstruct it. In the perfect scheme, the size of a share must be at least that of the secret. On the other hand, ramp secret sharing schemes allow shares to be smaller than the size of the secret. They can be much more efficient than perfect schemes (because of the size of the shares).

Security? There are two important parameters, the privacy parameter t and the reconstruction parameter r. Any party having t or less shares has no information about the secret, and any party having r or more shares can recover the secret. For perfect schemes, one has that r is equal to $t+1$. However, for ramp schemes one has a grey area between r and t of shares that has some partial information about the secret. The threshold gap, defined as the quantity $r-t$, is desired to be small. We obtained a family of bounds for the threshold gap which are tighter than the previously known bounds in [7].

Computing the security parameters? The minimum distance (of one of the codes and the dual of the other one) gives a bound on r and t. The exact value is given by the first relative generalized Hamming weight (RGHW) [35], of the pair of nested codes used. Moreover, if we want to completely characterize the security of a secret sharing scheme, we need all the RGHWs [33, 29]. These weights are an extension of the definition of minimum distance for a pair of codes and they are very difficult to compute for arbitrary codes. We have been able to estimate RGHWs of one-point algebraic geometric codes [29] and considered asymptotic families of secret sharing schemes with excellent parameters by using towers of function fields [27, 28].

Challenge? One challenge is to obtain linear codes that provide efficient and fast implementations over a binary finite field. Moreover, a small threshold gap is desirable. The other challenge is to focus in partial privacy, allowing that a negligible amount of information is leaked, one can obtain more efficient implementations.

3. Quantum codes

Motivation? Quantum computers are based on the principles of quantum mechanics and use subatomic particles (qubits) to hold memory. The construction of efficient devices of this type would have important consequences because of their computing capabilities. In fact, as Shor proved, they would break most of the known cryptographic systems. There is no known efficient quantum computer but it seems that these computers could appear in a short space of time [8]. Despite quantum mechanical systems being very sensitive to disturbances and arbitrary quantum states being unable to be replicated, error correction is possible [38].

Construction? An important class of quantum error-correcting codes are stabilizer codes, which can be derived from classical codes. An interesting particular case is the renowned CSS construction which uses a classical linear code containing its dual [4, 32]. This construction can be improved using two nested codes, which is known as Steane's enlargement [30, 22]. Many works have concentrated on considering quantum MDS codes [9], but the length of a quantum MDS code is bounded by the square of the field size plus one.

Algebraic constructions? J-affine variety codes are a family of affine-variety codes that allow us to consider subfield subcodes by studying cyclotomic cosets, where we consider our enlargement and subfield subcodes of affine variety codes [21, 22, 17]. Our research extends the univariate construction of BCH quantum codes [34] to several variables and uses self-orthogonality with respect to Hermitian inner product as well, obtaining a wider variety of parameters. We have also considered evaluation codes at the trace roots to construct quantum codes [23].

Extension? This theory has been extended to asymmetric quantum error-correcting codes which are useful in a model where the probabilities of qubit-flip and phase-shift errors are different [41]. This generalization is motivated by experiments that show that dephasing will happen more frequently than relaxation. From a pair of nested linear codes one can construct an asymmetric quantum code by the CSS construction for asymmetric quantum codes [4, 32], having a code with two different error correction capabilities for the two different kind of errors. Entanglement-assisted quantum error-correcting codes (EAQECCs) [3, 19] enable correction of more errors under certain conditions and they are defined from classical linear codes with less restrictive conditions about self-orthogonality than the CSS construction. In fact, we can consider an arbitrary linear code. EAQECCs make use of pre-existing entanglement between transmitter and receiver to correct more errors. Furthermore, these two extensions were combined to define Asymmetric Entanglement-Assisted Quantum Error-Correcting Codes in [20].

Relation to secret sharing? As we showed in [18], these two error correction capabilities are given by the first relative Hamming weight of the code pair and their duals. Hence, these two values are strongly related to the privacy and reconstruction parameters of a secret sharing scheme constructed from the same pair of codes.

Challenge? As for classical linear codes, the challenge is to construct codes that, apart from correcting many errors using as few extra symbols as possible, can also provide fast en- and decoding algorithms.

4. Multi-party computation

What is it? Multi-party computation studies the case where a group of persons, each holding an input for a function, wants to compute the output of the function, without having each individual reveal his or her input to the other parties. Multi-party computation is possible from secret sharing schemes [12], and hence from coding theory. Component-wise products of linear codes have been studied for various purposes in recent decades. For instance, to attack some variants of the McEliece [37] and to decode Reed-Solomon codes. They are also useful for multi-party computation.

Construction? To evaluate a boolean circuit using a multiparty computation protocol, one of the best known protocols at present are MiniMac [14] and its successor TinyTable [13]. They use a linear binary code C, which should prevent cheating. The probability that a cheating player is caught depends on the minimum distance of C^{*2}, the square code of linear code [40], meaning that a high distance on the square will give a higher security. Simultaneously, it would be beneficial to have a high dimension on the code C to reduce the communication cost. Additionally, if the minimum distance of the dual of C and C^{*2} are greater than or equal to $t+2$, then C can be used to construct a t-strongly multiplicative secret sharing scheme. Such a secret sharing scheme is enough to construct an information theoretic secure secret sharing scheme if at most t players are corrupted.

Challenge? These applications show the importance of finding linear codes,in which both the code itself and the square has good parameters. To be more specific, that the dimension of C, the minimum distance of the dual of C and the minimum distance of C^{*2} are simultaneously high relative to the length of the codes. Choosing a random linear code, with dimension linear in the length, will, with high probability, give a reasonable minimum distance. However, this does not hold for the square code [6]. Hence, constructing good

square codes is a very difficult problem. Nevertheless, good square codes exist, since there exists an asymptotic family of codes with the previous property [39]. The best binary construction available in the literature is the one in [5] obtained from cyclic codes, but their constellation is quite limited. Given a designed minimum distance d we computed in [24] an affine variety code C such that $d(C^{*2}) \geq d$ and the dimension of C is high. The best constructions we proposed mostly come from hyperbolic codes. Nevertheless, for small values of d, they come from weighted Reed–Muller codes.

5. Private information retrieval

What is it? A Private Information Retrieval (PIR) scheme is a protocol that allows retrieving an item from a database server without revealing which item is retrieved, i.e., protecting a user from a curious database operator. It is a recent research topic, initiated by [11], since the usual focus in cybersecurity has been on protecting the information of the database itself, but not on protecting the user from the database administrator or owner. This is currently particularly important where users' privacy is at risk and it helps dissidents, citizens of oppressive regimes, and internet users to remain anonymous. Further applications for citizens and companies include an investor that queries the stock-market database for the value of a certain stock, who may wish to keep private the stock he is interested in.

Construction? The best PIR protocols arise from using a pair of linear codes where the database is stored in a distributed data storage. There are several proposals in literature, but the best construction is currently provided by [43] for a situation where there is no active adversary. It was extended in [16, 44] for addressing a more complete and more realistic picture: they consider that the servers may collude (ie. they communicate), that there are byzantine adversaries (adversaries that leak and modify the information) and that the servers may be non-responding (they are broken, or the communication fails). The construction is based on generalized Reed-Solomon codes, namely a pair codes, the storage code C and the query code D. The performance and security are determined by the component-wise product code of these two codes, $C * D$ [40].

Challenge? The best PIR schemes available are implemented over a large finite field. There is a proposal for using binary Reed-Muller codes [15], since considering a more efficient family of codes is desirable. In particular, a code over a small finite field, since generalized Reed-Solomon codes require a high finite field size. We have recently improved the performance of the binary PIR schemes given in [15] by using binary cyclic codes [2].

References

[1] G. R. Blakley and Catherine Meadows, *Security of ramp schemes*, Advances in cryptology (Santa Barbara, Calif., 1984), Lecture Notes in Comput. Sci., vol. 196, Springer, Berlin, 1985, pp. 242–268.
[2] Seyma Bodur, Edgar Martínez-Moro, and Diego Ruano, *Private information schemes using cyclic codes*, arXiv preprint arXiv:2111.09060 (2021).
[3] Todd Brun, Igor Devetak, and Min-Hsiu Hsieh, *Correcting quantum errors with entanglement*, science **314** (2006), no. 5798, 436–439.
[4] A Robert Calderbank and Peter W Shor, *Good quantum error-correcting codes exist*, Physical Review A **54** (1996), no. 2, 1098.
[5] Ignacio Cascudo, *On squares of cyclic codes*, IEEE Trans. Inform. Theory **65** (2019), no. 2, 1034–1047.
[6] Ignacio Cascudo, Ronald Cramer, Diego Mirandola, and Gilles Zémor, *Squares of random linear codes*, IEEE Trans. Inform. Theory **61** (2015), no. 3, 1159–1173.

[7] Ignacio Cascudo, Jaron Skovsted Gundersen, and Diego Ruano, *Improved bounds on the threshold gap in ramp secret sharing*, IEEE Trans. Inform. Theory **65** (2019), no. 7, 4620–4633.
[8] Davide Castelvecchi, *Quantum computers ready to leap out of the lab in 2017*, Nature **541** (2017), no. 7635.
[9] Bocong Chen, San Ling, and Guanghui Zhang, *Application of constacyclic codes to quantum MDS codes*, IEEE Trans. Inform. Theory **61** (2015), no. 3, 1474–1484.
[10] Hao Chen, Ronald Cramer, Shafi Goldwasser, Robbert de Haan, and Vinod Vaikuntanathan, *Secure computation from random error correcting codes*, Advances in cryptology—EUROCRYPT 2007, Lecture Notes in Comput. Sci., vol. 4515, Springer, Berlin, 2007, pp. 291–310.
[11] Benny Chor, Oded Goldreich, Eyal Kushilevitz, and Madhu Sudan, *Private information retrieval*, J. ACM **45** (1998), no. 6, 965–982. MR 1678848
[12] Ronald Cramer, Ivan Bjerre Damgård, and Jesper Buus Nielsen, *Secure multiparty computation and secret sharing*, Cambridge University Press, 2015.
[13] Ivan Damgård, Jesper Buus Nielsen, Michael Nielsen, and Samuel Ranellucci, *The tinytable protocol for 2-party secure computation, or: Gate-scrambling revisited*, Annual International Cryptology Conference, Springer, 2017, pp. 167–187.
[14] Ivan Damgård and Sarah Zakarias, *Constant-overhead secure computation of boolean circuits using preprocessing*, Theory of Cryptography Conference, Springer, 2013, pp. 621–641.
[15] Ragnar Freij-Hollanti, Oliver W. Gnilke, Camilla Hollanti, Anna-Lena Horlemann-Trautmann, David Karpuk, and Ivo Kubjas, *t-private information retrieval schemes using transitive codes*, IEEE Trans. Inform. Theory **65** (2019), no. 4, 2107–2118.
[16] Ragnar Freij-Hollanti, Oliver W. Gnilke, Camilla Hollanti, and David A. Karpuk, *Private information retrieval from coded databases with colluding servers*, SIAM J. Appl. Algebra Geom. **1** (2017), no. 1, 647–664.
[17] Carlos Galindo, Olav Geil, Fernando Hernando, and Diego Ruano, *On the distance of stabilizer quantum codes from J-affine variety codes*, Quantum Inf. Process. **16** (2017), no. 4, Paper No. 111, 32.
[18] ———, *Improved constructions of nested code pairs*, IEEE Trans. Inform. Theory **64** (2018), no. 4, part 1, 2444–2459.
[19] Carlos Galindo, Fernando Hernando, Ryutaroh Matsumoto, and Diego Ruano, *Entanglement-assisted quantum error-correcting codes over arbitrary finite fields*, Quantum Inf. Process. **18** (2019), no. 4, Paper No. 116, 18.
[20] ———, *Asymmetric entanglement-assisted quantum error-correcting codes and bch codes*, IEEE Access **8** (2020), 18571–18579.
[21] Carlos Galindo, Fernando Hernando, and Diego Ruano, *New quantum codes from evaluation and matrix-product codes*, Finite Fields Appl. **36** (2015), 98–120.
[22] ———, *Stabilizer quantum codes from J-affine variety codes and a new Steane-like enlargement*, Quantum Inf. Process. **14** (2015), no. 9, 3211–3231.
[23] ———, *Classical and quantum evaluation codes at the trace roots*, IEEE Trans. Inform. Theory **65** (2019), no. 4, 2593–2602.
[24] Ignacio García-Marco, Irene Márquez-Corbella, and Diego Ruano, *High dimensional affine codes whose square has a designed minimum distance*, Des. Codes Cryptogr. **88** (2020), no. 8, 1653–1672.
[25] Olav Geil, *Evaluation codes from an affine variety code perspective*, Advances in algebraic geometry codes, Ser. Coding Theory Cryptol., vol. 5, World Sci. Publ., Hackensack, NJ, 2008, pp. 153–180.
[26] Olav Geil and Tom Høholdt, *Footprints or generalized Bezout's theorem*, IEEE Trans. Inform. Theory **46** (2000), no. 2, 635–641.
[27] Olav Geil, Stefano Martin, Umberto Martínez-Peñas, Ryutaroh Matsumoto, and Diego Ruano, *On asymptotically good ramp secret sharing schemes*, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences **100** (2017), no. 12, 2699–2708.
[28] Olav Geil, Stefano Martin, Umberto Martínez-Peñas, and Diego Ruano, *Refined analysis of RGHWs of code pairs coming from garcia-stichtenoth's second tower*, Journal of Algebra Combinatorics Discrete Structures and Applications **4** (2017), no. 1, 37–47.

[29] Olav Geil, Stefano Martin, Ryutaroh Matsumoto, Diego Ruano, and Yuan Luo, *Relative generalized Hamming weights of one-point algebraic geometric codes*, IEEE Trans. Inform. Theory **60** (2014), no. 10, 5938–5949.
[30] Mitsuru Hamada, *Concatenated quantum codes constructible in polynomial time: efficient decoding and error correction*, IEEE Trans. Inform. Theory **54** (2008), no. 12, 5689–5704. MR 2596809
[31] Tom Høholdt, Jacobus H. van Lint, and Ruud Pellikaan, *Algebraic geometry codes*, Handbook of coding theory, Vol. I, II, North-Holland, Amsterdam, 1998, pp. 871–961.
[32] Avanti Ketkar, Andreas Klappenecker, Santosh Kumar, and Pradeep Kiran Sarvepalli, *Nonbinary stabilizer codes over finite fields*, IEEE Trans. Inform. Theory **52** (2006), no. 11, 4892–4914.
[33] Jun Kurihara, Ryutaroh Matsumoto, and Tomohiko Uyematsu, *Relative generalized rank weight of linear codes and its applications to network coding*, IEEE Trans. Inform. Theory **61** (2015), no. 7, 3912–3936.
[34] Giuliano Gadioli La Guardia, *On the construction of nonbinary quantum BCH codes*, IEEE Trans. Inform. Theory **60** (2014), no. 3, 1528–1535.
[35] Yuan Luo, Chaichana Mitrpant, A. J. Han Vinck, and Kefei Chen, *Some new characters on the wire-tap channel of type II*, IEEE Trans. Inform. Theory **51** (2005), no. 3, 1222–1229.
[36] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes. I*, North-Holland Mathematical Library, Vol. 16, North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977.
[37] Irene Márquez-Corbella, Edgar Martínez-Moro, Ruud Pellikaan, and Diego Ruano, *Computational aspects of retrieving a representation of an algebraic geometry code*, J. Symbolic Comput. **64** (2014), 67–87.
[38] Michael A. Nielsen and Isaac L. Chuang, *Quantum computation and quantum information*, Cambridge University Press, Cambridge, 2000.
[39] Hugues Randriambololona, *Asymptotically good binary linear codes with asymptotically good self-intersection spans*, IEEE Trans. Inform. Theory **59** (2013), no. 5, 3038–3045.
[40] ———, *On products and powers of linear codes under componentwise multiplication*, Algorithmic arithmetic, geometry, and coding theory, Contemp. Math., vol. 637, Amer. Math. Soc., Providence, RI, 2015, pp. 3–78. MR 3364442
[41] Pradeep Kiran Sarvepalli, Andreas Klappenecker, and Martin Rötteler, *Asymmetric quantum codes: constructions, bounds and performance*, Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences **465** (2009), no. 2105, 1645–1672.
[42] Adi Shamir, *How to share a secret*, Comm. ACM **22** (1979), no. 11, 612–613.
[43] Razane Tajeddine, Oliver W. Gnilke, and Salim El Rouayheb, *Private information retrieval from MDS coded data in distributed storage systems*, IEEE Trans. Inform. Theory **64** (2018), no. 11, 7081–7093.
[44] Razane Tajeddine, Oliver W. Gnilke, David Karpuk, Ragnar Freij-Hollanti, and Camilla Hollanti, *Private information retrieval from coded storage systems with colluding, Byzantine, and unresponsive servers*, IEEE Trans. Inform. Theory **65** (2019), no. 6, 3898–3906.

IMUVA-Mathematics Research Institute, Universidad de Valladolid
Email address: diego.ruano@uva.es

CONTRIBUTED TALKS

MORSE CELL DECOMPOSITION AND PARAMETRIZATION OF SURFACES FROM POINT CLOUDS

M. ALBERICH-CARRAMIÑANA, J. AMORÓS, F. COLTRARO, C. TORRAS, AND M. VERDAGUER

Abstract. An algorithm for the reconstruction of a surface from a point sample is presented. It proceeds directly from the point-cloud to obtain a cellular decomposition of the surface derived from a Morse function. No intermediate triangulation or local implicit equations are used, saving on computation time and reconstruction-induced artifices. No a priori knowledge of surface topology, density or regularity of its point sample is required to run the algorithm. The results are a piecewise parametrization of the surface as a union of Morse cells, suitable for tasks such as noise-filtering or mesh-independent reparametrization, and a cell complex of small rank determining the surface topology. The algorithm can be applied to smooth surfaces with or without a boundary, embedded in an ambient space of any dimension.

Introduction

Reconstruction of a surface in space from a sample of points on it is a question to which considerable attention has been devoted in the areas of Computational Geometry and Computer Graphics ([3]). The authors' goal is a fast algorithm for topology identification and parametrization of surfaces with boundary. These qualities were required for robotic handling of textiles, but are expected to make the algorithm fit to study higher dimensional algebraic varieties.

Differential Topology has tackled the piecewise parametrization problem for manifolds through Morse functions. Applying this idea directly to the sample point cloud of a surface was suggested by [5],[9], who propose an algorithm for point clouds with a known, homogeneous density of sampling. Cazals et al ([2]) propose a Morse decomposition scheme from point clouds sampling manifolds of any dimension. The complexity of their algorithm preserves the interest in simpler schemes for low dimension.

In this study, the authors report a complete Morse cell decomposition algorithm for surfaces of any topology, with or without a boundary, which can be applied to sample point clouds without a priori knowledge of sampling density or regularity, or of surface topology. It can be applied to surfaces in any ambient dimension. We use the gradient flows of [5],[9] as the starting point, but then detect saddle points and their Morse cells by studying the level sections of these flows.

Date: 2022/3/2.

The authors have been supported by Clothilde (ERC-AdG-741930), and PID2019-103849GB-I00 of MCIN/AEI/10.13039/501100011033.

The talk at the meeting EACA 2022 was given by the third author.

Contents

1. From Morse theory for manifolds...

Let M be a smooth compact manifold. A map $f : M \to \mathbb{R}$ is *Morse* if it is $\mathcal{C}^2$, has only finitely many critical points, and at all of these the Hessian $d^2 f(P)$ is nondegenerate. Classical Morse theory (see [7]) shows that a generic Morse function f induces, through its gradient flow, two decompositions of the manifold M:
1. *As a CW complex* (see [8]): each critical point of f, together with its unstable manifold for the vector field $-\nabla f$, forms a cell which is topologically a ball, whose boundary attaches to lower-dimensional cells. A global piecewise parametrization of M is achieved, as well as a Morse-Smale complex, with the critical points of f as a basis, computing the singular homology of M.
2. *As level sets*: M is foliated by the level sets $f^{-1}(c)$. For regular values c these level sets are submanifolds of M with codimension 1, with $f^{-1}(c_1) \cong f^{-1}(c_2)$ if no critical value of f lies between c_1 and c_2. The transformation of the level set when c crosses a critical value of f is a surgery ([7]).

The success of Morse theory lies in the fact that Morse functions, and the Morse-Smale transversality required for the above analysis, are generic among $\mathcal{C}^2$ maps from M to $\mathbb{R}$. For instance, the height function in a random direction in $\mathbb{R}^N$ has a probability of 1 of being a Morse-Smale function. Morse theory also extends to manifolds with boundary ([6]).

2. ...to point clouds

Let $X \subset \mathbb{R}^N$ be a point cloud sampling a compact surface S, possibly with boundary. Select neighbours of each point P in the sample. Choose a unit vector $v \in \mathbb{R}^N$ such that the height function $f(x) = x \cdot v$ has different values in all points of X, and define the gradient (or *upwards*), resp. -gradient (or *downwards*) flows of f by sending every point P in the cloud to its neighbour that maximizes the slope of growth of f, resp. makes f decrease with the most negative slope. Points where f cannot grow, resp. decrease, are local maxima, resp. minima of f in X.

Interpret the downwards flow of f on X as a graph with edges connecting each point in the cloud to its downwards neighbour. The intersections of this graph with the hyperplane $x \cdot v = c$ are point samples for the level set $f^{-1}(c)$ on the original surface S, with some noise added by the linear interpolation. This level set consists of finitely many simple curves, either closed or with edges in the boundary of S. The curves can be reconstructed by any standard procedure.

Perform these level set intersections at n equispaced levels $c_i = c_0 + i \cdot h$ ranging from $c_0 = \min f(X)$ to $c_n = \max f(X)$. The number of level sections n must be selected, and the idea is that all surface handles whose range in height is h or greater will be detected. Changes in the topology of the level set are now variations in the number of curves. Each surgery in the level set induced by its going over a saddle point of f can be tracked by two pairs of neighbours in the sample of a level set which end up in different connected components of the other level set after upwards or downwards flow.

Following the downwards flow of the 4 points in these 2 pairs, and their pairing according to closeness, the level at which the pairing changes locates the saddle point. The unstable variety of this saddle point for the flow of $-\nabla f$ is approximated by taking the two pairs of neighbouring points at the level of f immediately below the saddle point, and averaging the

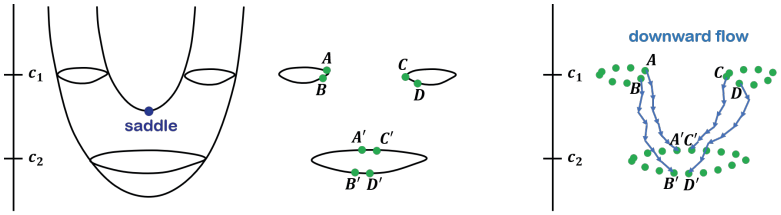


FIGURE 1. Change in level set when crossing a critical value in a surface (left) and point cloud (right): note the change in neighbours among the 4 marked points after the flow.

downward orbits of each pair (see Figure 1). These computations have a margin of error $O(d)$, where d is the local variation of height among neighbouring cloud points.

3. IMPLEMENTATION

The first and costliest step is the identification of a set of neighbours of each point in the cloud. Merging usual criteria, we take 2 points as neighbours when (i) their Voronoi cells in the decomposition of ambient space $\mathbb{R}^N$ induced by X are adjoining, and (ii) each point is among the k nearest neighbours of the other in the cloud, with $k \in [6, 12]$ as suggested by sphere packing on surfaces.

The boundary is identified among points in the cloud by PCA analysis of tangent spaces at each point using its neighbours (as in [1]). Neighbours of a boundary point cluster in a semispace.

Curve reconstruction with the NN-Crust algorithm of T. Dey ([3]) is used for boundary parametrization, and afterwards for level set reconstruction when we intersect the gradient flow graph with level hyperplanes.

Once the saddle points of the height function and their (un)stable varieties have been found, the piecewise parametrization for the entire surface follows: 0-cells are the local minima, 1-cells have been parametrized at saddle point detection, and each 2-cell can be parametrized from the tree formed in it by the upwards flow to its unique maximum, e.g. with the shape-preserving algorithm of Floater ([4]).

Finally, the boundary relations given by the downwards flow on the cells give us the Morse-Smale complex and singular homology of the surface S.

The complexity of the complete algorithm for a sample cloud of n points is $O(n \log(n))$. Figure 2 shows its Matlab implementation in a laptop PC applied to a 30.116-point sample from a torus, embedded in $\mathbb{R}^3$ along a (2,3)-toric knot. 2 local maxima, 2 local minima and 4 saddle points are correctly detected for the height function. A parametrization of the surface into 8 cells is found in 95" (of which 93" for the determination of neighbours).

4. CONCLUSIONS

The algorithm presented in this work successfully reconstructs a surface S by finding a Morse cellular decomposition from a cloud of sampled points. The advantages of this approach are:

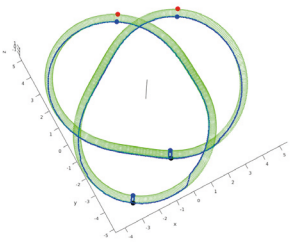


FIGURE 2. A sampled knotted torus: the black line is the direction of the height function; local maxima, resp. minima, are painted red, resp. black; saddle points are painted blue; their 1–cells are outlined in blue.

- A global piecewise parametrization of the surface is found, with a number of pieces O(1000) times smaller than that of sample points in typical examples.
- The topology of the surface can be deduced immediately from the cellular decomposition.
- The algorithm is robust: it always produces a surface, and it captures the topological features of the sampled surface with a size greater than the typical distance between sample points.
- In the presence of noise in the sample points position, the parametrization allows the use of a range of filtering techniques while preserving the surface topology.
- The algorithm can be applied to surfaces in $\mathbb{R}^N$ for any ambient dimension N.

The authors expect to extend this algorithm to the reconstruction of higher dimensional manifolds by iterating the hyperplane sections, reconstructing the manifold from lower dimensional slices. A further extension would be to study of real algebraic varieties of any dimension, where point cloud samples can be obtained from their equations and refined where necessary. We anticipate this will lead our method to detect a Whitney stratification, and the Morse cellular decomposition after [6] of the variety, by purely numerical methods.

REFERENCES

[1] Y. Cao, D. Li, H. Sun, A. Assadi, S. Zhang, *Efficient Weingarten Map and Curvature Estimation on Manifolds*. arxiv:stat.ML.1905.10725
[2] F. Cazals, A. Roth, C. Robert, M. Christian, *Towards Morse Theory for Point Cloud Data*, Research Report RR-8331, INRIA. 2013, pp.37.
[3] T. Dey, *Curve and surface reconstruction. Algorithms with mathematical analysis*. CUP, 2006.
[4] M. Floater, *Parametrization and smooth approximation of surface triangulations*, Computer Aided Geometric Design **14** (1997) 231–250.
[5] J. Gao, R. Sarkar, X. Zhu, *Morse-Smale Decomposition, Cut Locus and Applications in Wireless Sensor Networks*, `http://page.mi.fu-berlin.de/sarkar/papers/morse-boundary-theory.pdf` 2008.
[6] M. Goresky, R. MacPherson, *Stratified Morse Theory*. Springer Verlag, 1988.
[7] M. Hirsch, *Differential Topology*. Springer Verlag, 1976.
[8] J. Munkres, *Elements of Algebraic Topology*. Addison-Wesley, 1984.
[9] X. Zhu, R. Sarkar, J. Gao, *Topological Data Processing for Distributed Sensor Networks with Morse-Smale Decomposition*, IEEE INFOCOM 2009 (pp. 2911-2915).

Institut de Robòtica i Informàtica Industrial, CSIC-UPC. Barcelona, Spain
E-mail address: `fcoltraro@iri.upc.edu`

THE MINIMAL MODEL OF A SIMPLICIAL COMPLEX: AN ALGORITHM AND IMPLEMENTATION

ALQUEZAR-BAETA, C., MARCO BUZUNARIZ, M.A., AND MARTÍN-MORALES, J.

Abstract. We present an implementation in SageMath ([4]) of a new method to compute the minimal model of a simplicial complex. The method is a modification of the one provided for minimal models of GCDA's of finite type by Manero and Marco in [3] to deal in this particular case of algebras with infinite dimensional homogenous parts.

This method is presented for simplicial complexes but could be easily adapted for simplicial sets.

Introduction

Given a manifold, it is well known that its DeRham algebra encodes most of the differential structure (and hence also topological). In particular, the rational type is given by the minimal model of this algebra. For spaces that are not manifolds the same is true if we consider the minimal model of the A_{PL} algebra instead.

These algebras are in general too big to be handled computationally. However, if the space is represented by a triangulation, we can use the more manageable A_{PL} algebra of this simplicial complex.

The elements of this algebra are given by certain assignations of a (generally noncommutative) polynomial to each simplex, so they can be represented with a finite amount of information. That is, we can perform concrete computations in this algebra.

More precisely, given a simplicial complex K, an element of the algebra $A_{PL}(K)$ can be represented as a tuple $(P_\sigma)_{\sigma\in K}$, where, for each simplex σ of dimension n, P_σ is a (noncommutative) polynomial in the algebra

$$(A_{PL})_n = \frac{\bigwedge(t_0,\dots,t_n,y_0,\dots,y_n)}{\langle\sum t_i - 1, \sum y_j\rangle}$$

where t_i have degree zero, and y_i have degree one. This assignation must be compatible with the face maps

$$\partial_i(t_k) = \begin{cases} t_k, & k<i \\ 0 & k=i \\ t_{k-1}, & k>i \end{cases} \qquad \partial_i(y_k) = \begin{cases} y_k, & k<i \\ 0 & k=j \\ y_{k-1}, & k>i \end{cases}$$

in the sense that the i-th face of P_σ must coincide with the assignation to the i'th face of σ.

The authors were partially supported by PID2020-114750GB-C31, E22_20R: Álgebra y Geometría, y BES-2017-079979.

The third author was partially supported by FQM-333.

The talk at the EACA 2022 Meeting was given by the second author.

With this representation, this is a CDGA with algebra operations and the gradings induced by the underlying algebras $(A_{PL})_n$, and the differential is induced by

$$d(t_i) = y_i, \quad d(y_i) = 0.$$

However, the algebra itself is not of a finite type: for every degree we have an infinite dimensional vector space. Because of this, the algorithm proposed by Manero and Marco in [3] cannot be used.

However, it can be adapted for this particular case.

1. Algorithm for the minimal model of a simplicial complex

We will use some auxiliary functions that will be outlined now. First, we define an integration map

$$\int_n : (A_{PL})^n_n \longrightarrow \mathbb{Q}$$

given by

$$\int_n t_1^{k_1} t_2^{k_2} \dots t_n^{k_n} y_1 \dots y_n := \frac{k_1! k_2! \dots k_n!}{(k_1 + \dots + k_n + n)!}$$

which induces a global map to the simplicial cochains

$$\oint : A_{PL}(K) \to C^*(K).$$

We also need a section of this map

$$\Theta : C^*(K) \to A_{PL}(K),$$

which can be computed by first lifting a single number assigned to a single simplex σ, to a polynomial P_σ, and then propagating this polynomial to the surrounding simplices, so the final assignation satisfies the face restrictions.

Finally, using linear algebra, we will also use a partial function

$$S : (A_{PL}(K))^{n+1} \to (A_{PL}(K))^n$$

that provides a section for the differential.

Now, the algorithm runs as follows:

The input is a simplicial complex.

The output will be a map $M \to A_{PL}(K)$ from a minimal Sullivan algebra, represented by a list of triplets $(x_i^d, d(x_i^d), \varphi(x_i^d))$, where

- x_i^d is a generator of M of degree d.
- $d(x_i^d)$ is a (graded commutative) polynomial on the previous generators.
- $\varphi(x_i^d)$ is an element of $(A_{PL}(K))^d$.

The algorithm keeps adding triplets to the list. With an abuse of notation, we will refer to the model obtained so far in each moment as M.

Start with an empty list, and then repeat the following loop.

(1) Assume we have a map $\phi : M \to A_{PL}(K)$ that induces an isomorphism in cohomology up to degree $k-1$.

(2) This step must be repeated until φ_k^* is injective at degree k.
Let $[z_0^k], \ldots, [z_{l_k}^k]$ be a basis of the kernel of $\oint^* \circ \phi_k^*$.
Compute $C_j^k = \varphi(z_j^k) \in A_{PL}(K)^k$ and $B_j^{k-1} = S(C_j^k)$.
Add the generators y_i^{k-1} with $\varphi(y_i^{k-1}) = B_i^{k-1}$ and $d_M(y_i^{k-1}) = z_i^k$ to the list.
(3) Take a basis $[a_0^k], \ldots, [a_{l_k}^k]$ of the complement of the image of $\oint^* \circ \phi_k^*$.
Add to the list new generators of degree k of M, $\{x_0^k, \ldots, x_{l_k}^k\}$, with $d(x_i^k) = 0$ and $\phi(x_i^k) = \Theta(A_i^k)$.

2. Example

In this section, we show the example of computing the minimal model of $\mathbb{CP}^2$. The triangulation used for that purpose is the one available at SageMath as a simplicial complex, composed by 9 vertices and 36 facets, all of dimension 4. Each simplex of dimension n is represented as an $(n+1)$-tuple of vertices. We denote this simplicial complex by K. The full list of facets is:

$(2,4,5,8,9)$	$(1,2,4,5,9)$	$(3,4,5,7,8)$	$(2,5,6,7,8)$	$(1,4,6,7,8)$	$(3,5,6,7,9)$
$(1,3,4,7,8)$	$(1,2,6,7,8)$	$(3,4,6,8,9)$	$(2,3,4,5,8)$	$(1,3,4,5,6)$	$(2,3,6,7,9)$
$(2,4,6,7,9)$	$(1,2,4,5,6)$	$(1,2,5,8,9)$	$(1,2,4,7,9)$	$(1,2,4,6,7)$	$(4,5,7,8,9)$
$(1,2,3,7,9)$	$(1,3,4,6,8)$	$(1,2,3,8,9)$	$(2,3,4,5,6)$	$(5,6,7,8,9)$	$(1,2,3,7,8)$
$(1,2,5,6,8)$	$(1,4,5,7,9)$	$(2,3,4,6,9)$	$(1,5,6,8,9)$	$(2,3,4,8,9)$	$(1,3,5,6,9)$
$(2,3,5,7,8)$	$(1,3,4,5,7)$	$(1,3,5,7,9)$	$(2,3,5,6,7)$	$(4,6,7,8,9)$	$(1,3,6,8,9)$

We have computed the minimal model of K with our SageMath package giving rise to the following CDGA:

```
sage: print(model)
Commutative Differential Graded Algebra with generators
('x2_0', 'y5_0') in degrees (2, 5) over Rational Field
with differential:
   x2_0 --> 0
   y5_0 --> x2_0^3
```

This means that the minimal model of the complex plane $\mathbb{CP}^2$ is $M = \langle x_0^2, y_0^5 \rangle$ and $d(y_0^5) = (x_0^2)^3$. The corresponding morphism $\varphi : M \to A_{PL}(K)$ is also obtained with our implementation. The image of x_0^2 is determined by the nonzero values of the following faces:

$$
\begin{array}{lcl}
(2,3,4,5,6) & \to & 2y_1y_2 + 2y_1y_3 + 2y_1y_4 \\
(2,3,4,5,8) & \to & 2y_1y_2 + 2y_1y_3 - 2y_2y_4 \\
(2,3,4,6,9) & \to & 2y_1y_2 + 2y_1y_3 - 2y_3y_4 \\
(2,3,4,8,9) & \to & 2y_1y_2 - 2y_2y_3 \\
(2,3,5,6,7) & \to & 2y_1y_2 + 2y_1y_3 - 2y_2y_4 \\
(2,3,5,7,8) & \to & 2y_1y_2 - 2y_2y_3 \\
(2,3,6,7,9) & \to & 2y_1y_2 - 2y_2y_4 \\
(2,4,5,8,9) & \to & -2y_1y_3 \\
(2,4,6,7,9) & \to & -2y_2y_4
\end{array}
$$

$$\begin{array}{rcl}(2,5,6,7,8) & \to & -2y_1y_3\\ (3,4,5,7,8) & \to & 2y_2y_4\\ (3,4,6,8,9) & \to & 2y_1y_4\\ (3,5,6,7,9) & \to & 2y_2y_3\\ (4,5,7,8,9) & \to & 2y_1y_3 - 2y_3y_4\\ (4,6,7,8,9) & \to & -2y_1y_4 - 2y_3y_4\\ (5,6,7,8,9) & \to & 2y_1y_2 - 2y_2y_3\end{array}$$

and the element associated with y_0^5 is the zero element in $(A_{PL}(K))^5$.

References

[1] Y. Felix, S. Halperin, J.C. Thomas, *Rational homotopy theory*, Graduate Texts in Mathematics, 205. Springer-Verlag, New York, 2001.

[2] A. Garvin, R. Gonzalez-Diaz, M.A. Marco and B. Medrano, *Making Sullivan algebras minimal through chain contractions*, Mediterr. J. Math. (2021), No 43, 1660–5446

[3] V. Manero and M.A. Marco-Buzunáriz, *Effective computation of degree bounded minimal models of GCDAs*, J. Softw. Algebra Geom. (2020), No 1, 25–39

[4] The Sage Developers, the Sage Mathematics Software System (Version 9.5), 2022, `https://www.sagemath.org`.

Universidad de Zaragoza/IUMA
Email address: `alquezar@unizar.es`

Universidad de Zaragoza/IUMA
Email address: `mmarco@unizar.es`

Universidad de Zaragoza/IUMA
Email address: `jorge.martin@unizar.es`

THIRD-ORDER MOMENT VARIETIES OF LINEAR NON-GAUSSIAN GRAPHICAL MODELS

CARLOS AMÉNDOLA, MATHIAS DRTON, ALEXANDROS GROSDOS, ROSER HOMS, AND ELINA ROBEVA

Abstract. In this work we study linear non-Gaussian graphical models from the perspective of algebraic statistics. These are acyclic causal models in which each variable is a linear combination of its direct causes and independent noise. The underlying directed causal graph can be identified uniquely via the set of second and third order moments of all random vectors that lie in the corresponding model. Our focus is on finding the algebraic relations among these moments for a given graph. We show that when the graph is a polytree these relations form a toric ideal. We construct explicit matrices associated to treks in the graph. Their entries are the covariances and third order moments, and their 2-minors define our model set-theoretically, and provide a generating set for the vanishing ideal of the model. Finally, we describe the polytopes of third order moments.

Introduction

Featuring prominently in a wide variety of applications, directed graphical models [**?**] capture intuitive cause-effect relations among a set of random variables by hypothesizing that each variable is a noisy function of its causes. For a number of statistical tasks, such as model selection, it has proven useful to obtain insights about the algebraic structure of the moments of the joint distributions in the graphical model for a given graph [**?**]. A prominent example are results on algebraic relations among second moments, i.e., covariances, in models that postulate linear functional relationships among the variables [**?**]. The results available include in particular, a characterization of the vanishing of subdeterminants of the covariance matrix, which covers conditional independence in Gaussian models as a special case. In contrast to earlier work in algebraic statistics, we present here a first systematic study on algebraic relations that also involve higher moments of such a model.

Let $G = (V, E)$ be a directed acyclic graph (DAG), and let $(X_i,\, i \in V)$, be a collection of random variables that represent statistical observations indexed by the vertices in V. A vertex $j \in V$ is a parent of vertex i if there is an edge pointing from j to i, i.e., if $(j, i) \in E$ which we also write as $j \to i \in E$. We denote the set of all *parents* of i by $\mathrm{pa}(i)$. The graph G gives rise to the *linear structural equation model* consisting of the joint distributions of all random vectors $X = (X_i, i \in V)$ such that

$$X_i = \sum_{j \in \mathrm{pa}(i)} \lambda_{ji} X_j + \varepsilon_i, \quad i \in V, \tag{1}$$

The first four authors were supported by the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (Grant agreement No. 883818).

The fifth author was supported by NSERC Discovery Grant (DGECR-2020-00338).

The talk at the EACA 2022 meeting was given by the third author.

Contents

where the ε_i are mutually independent random variables representing stochastic errors. The errors are assumed to have expectation $\mathbb{E}[\varepsilon_i] = 0$, finite variance $\omega_i^{(2)} = \mathbb{E}[\varepsilon_i^2] > 0$, and a finite third moment $\omega_i^{(3)} = \mathbb{E}[\varepsilon_i^3]$. No other assumption about their distribution is made and, in particular, the errors need not be Gaussian. The coefficients λ_{ji} in (1) are unknown real-valued parameters, and we fill them into a matrix $\Lambda = (\lambda_{ji}) \in \mathbb{R}^{V\times V}$ by adding a zero entry when $(j,i) \notin E$. We denote the set of all such sparse matrices as $\mathbb{R}^E$.

The model. The covariance matrix S and the third moment tensor T of X are given by

$$S = (s_{ij}) = (I-\Lambda)^{-T}\Omega^{(2)}(I-\Lambda)^{-1},$$
$$T = (t_{ijk}) = \Omega^{(3)} \bullet (I-\Lambda)^{-1} \bullet (I-\Lambda)^{-1} \bullet (I-\Lambda)^{-1},$$

where $\Omega^{(2)}$ is a diagonal matrix in the set $PD(V)$ of positive-definite matrices and similarly $\Omega^{(3)} \in \mathrm{Sym}_3(V)$ is a diagonal symmetric tensor. Here $\bullet$ denotes the Tucker product (see [**?**]).

Let $G = (V, E)$ be a DAG. The *third-order moment model* of G is the set $\mathcal{M}^{\leq 3}(G)$ that comprises all pairs of covariance matrices and third moment tensors that are realizable under the linear structural equation model given by G. That is,

$$\mathcal{M}^{\leq 3}(G) = \big\{\big((I-\Lambda)^{-T}\Omega^{(2)}(I-\Lambda)^{-1},\ \Omega^{(3)} \bullet (I-\Lambda)^{-1} \bullet (I-\Lambda)^{-1} \bullet (I-\Lambda)^{-1}\big) : \\ \Omega^{(2)} \in PD(V) \text{ diagonal},\ \Omega^{(3)} \in \mathrm{Sym}_3(V) \text{ diagonal},\ \Lambda \in \mathbb{R}^E\big\}.$$

Furthermore, the *third-order moment ideal* of G is the ideal $\mathcal{I}^{\leq 3}(G)$ of polynomials in the entries $S = (s_{ij})$ and $T = (t_{ijk})$ that vanish when $(S, T) \in \mathcal{M}^{\leq 3}(G)$.

In this work, we fully explain the situation regarding models $\mathcal{M}^{\leq 3}(G)$ in the case where G is a polytree, i.e., a directed acyclic graph whose underlying undirected graph is a tree.

1. Simple Trek Parametrization

We now give the definition of the concept of *multitrek* introduced in [**?**].

Definition 1.1. A *k-trek* between k vertices $i_1, \ldots, i_k$ is an ordered collection of directed paths $\tau = (P_1, \ldots, P_k)$ where P_r has sink i_r and they all share the same source v. We call v the *top* of the trek and denote it by $\mathrm{top}(\tau)$. A k-trek is called *simple* if its top node is the only node lying on all the k directed paths that form the trek. We denote the set of simple k-treks between $i_1, \ldots, i_k$ by $\mathcal{T}(i_1, \ldots, i_k)$.

The statistical significance of 2-treks is that they provide a combinatorial way to parametrize covariance matrices through what is known as the trek rule. This extends analogously to third-order moment tensors via 3-treks.

Furthermore, an advantage of working with DAGs is that one can simplify the description given by the trek rule by focusing only on simple treks. In [**?**, Section 2] it is shown that simple 2-treks give a different parametrization of the covariance matrix, by introducing a new set of indeterminates a_i for each vertex in the graph defined by

$$a_i := \sum_{l_1 \in pa(i)} \sum_{l_2 \in pa(i)} \lambda_{l_1,i}\lambda_{l_2,i}s_{l_1,l_2} + \omega_i^{(2)}. \tag{2}$$

This triangular, and thus invertible, transformation allows us to recursively pass from the diagonal entries in the matrix $\Omega^{(2)}$ to the a_i. The same is true for the entries of the tensor $\Omega^{(3)}$, via an analogous transformation. We therefore obtain the shorter *simple trek rule parametrization* induced by the polynomial ring map

$$\begin{aligned}\phi_G : \quad \mathbb{C}[s_{ij}, t_{ijk} \mid 1 \le i \le j \le k \le n] &\to \mathbb{C}[a_i, b_i, \lambda_{ij} \mid i \to j \in E], \\ s_{ij} &\mapsto \sum_{\tau \in \mathcal{T}(i,j)} a_{\mathrm{top}(T)} \prod_{k \to l \in \tau} \lambda_{kl}, \\ t_{ijk} &\mapsto \sum_{\tau \in \mathcal{T}(i,j,k)} b_{\mathrm{top}(T)} \prod_{m \to l \in \tau} \lambda_{ml}.\end{aligned}$$

This generalizes the corresponding construction in [?], and we can analogously prove:

Proposition 1.2 (Simple trek rule)**.** *Let $G = (V, E)$ be a DAG, and let ϕ_G be the ring morphism above. Then the map ϕ_G induces a parametrization of the model $\mathcal{M}^{\le 3}(G)$, and, therefore, $\mathcal{I}^{\le 3}(G) = \ker \phi_G$.*

In case the graph G is a *polytree*, the simple trek parametrization simplifies to a monomial map as $\mathcal{T}(i_1, \ldots, i_k)$ has at most one element: the unique simple k-trek between $i_1, \ldots, i_k$, if it exists. This implies

Corollary 1.3. *If G is a polytree, then the ideal $\mathcal{I}^{\le 3}(G)$ is toric.*

2. Low-Rank Trek-Matrices

In this section we find equations defining the model $\mathcal{M}^{\le 3}(G)$ when G is a polytree. We also give generators of the corresponding ideal.

Definition 2.1. Let G be a polytree. Let $i, j \in V$ be two vertices such that a 2-trek between i and j exists. We define the *trek-matrix* between i and j as

$$A_{i,j} := \begin{pmatrix} s_{ik_1} & \cdots & s_{ik_r} & t_{i\ell_1 m_1} & \cdots & t_{i\ell_q m_q} \\ s_{jk_1} & \cdots & s_{jk_r} & t_{j\ell_1 m_1} & \cdots & t_{j\ell_q m_q} \end{pmatrix},$$

where

- $k_1, \ldots, k_r$ are vertices such that $\mathrm{top}(i, k_a) = \mathrm{top}(j, k_a)$ for $a = 1, \ldots, r$, and
- $(l_1, m_1), \ldots, (l_q, m_q)$ are such that $\mathrm{top}(i, l_b, m_b) = \mathrm{top}(j, l_b, m_b)$ for $b = 1, \ldots, q$.

The next two results explain how to cut out the variety.

Lemma 2.2. *Let $G = (V, E)$ be a polytree, and $i, j \in V$. Then*

(a) *if there is no 2-trek between i and j, then $s_{ij} \in \mathcal{I}^{\le 3}(G)$, and for all $k \in V$ such that there is no 3-trek between i, j and k, we have that $t_{ijk} \in \mathcal{I}^{\le 3}(G)$.*

(b) *if there is an edge between i and j, the 2-minors of the trek-matrix $A_{i,j}$ lie in $\mathcal{I}^{\le 3}(G)$.*

Theorem 2.3. *Let G be a polytree and J be the ideal generated by the linear generators of $\mathcal{I}^{\le 3}(G)$ and the 2-minors of the matrices $A_{i,j}$ for $i \to j \in E$. Then,*

$$\mathcal{M}^{\le 3}(G) = \mathcal{V}(J) \cap (PD(V) \times \mathrm{Sym}_3(V)).$$

To obtain the generators of the ideal we need further polynomials arising from minors:

Theorem 2.4. *The third-order moment ideal $\mathcal{I}^{\leq 3}(G)$ of the model $\mathcal{M}^{(\leq 3)}(G)$ is generated by the linear generators of $\mathcal{I}^{\leq 3}(G)$ and the minors of matrices A_{ij} for all i, j such that a trek between them exists.*

To prove this theorem we show that this generating set is a Markov basis; for any binomial in $\mathcal{I}^{\leq 3}(G)$ we can apply an element of the set to reduce the distance between the two monomial terms.

3. Moment Polytopes

Given a polytree $G = (V, E)$, for any minimal 3-trek between i, j, k, we define the vector $e_{ijk} \in \mathbb{R}^{|V|+|E|}$ of exponents of the monomial $\phi_G(t_{ijk}) = b_{\mathrm{top}(i,j,k)} \prod_{l \to m \in \mathcal{T}(i,j,k)} \lambda_{lm} \in \mathbb{R}[b_l, \lambda_{lm}]$. Let $(\mathbf{z}, \mathbf{y})$ be the coordinates of e_{ijk}, where $\mathbf{z} = (z_l)_{l \in V}$ are the exponents of b_ℓ for $\ell \in V$ and $\mathbf{y} = (y_{lm})_{l \to m \in E}$ are the exponents of $\lambda_{\ell m}$ for $\ell \to m \in E$.

Definition 3.1. Given a polytree G, its associated third-order moment polytope is

$$P_G^{(3)} = \mathrm{conv}\left(e_{ijk} : i, j, k \text{ such that a 3-trek between } i,\ j \text{ and } k \text{ exists}\right).$$

The natural next step is to find the inequalities that cut out the polytope.

Theorem 3.2. *For a fully observed polytree G, the third-order moment polytope $P_G^{(3)}$ is the solution to the following set of equations and inequalities*

$$z_l \geq 0 \text{ for all } l \in V, \tag{3}$$

$$y_{lm} \geq 0 \text{ for all } l \to m \in E, \tag{4}$$

$$\sum_{l \in V} z_l = 1, \tag{5}$$

$$2z_l + \sum_{h \in pa(l)} y_{hl} - y_{lm} \geq 0 \text{ for all } m \text{ such that } l \to m \in E, \tag{6}$$

$$3z_l + \sum_{h \in pa(l)} y_{hl} - \sum_{m \in ch(l)} y_{lm} \geq 0 \text{ for all } l \in V. \tag{7}$$

Department of Mathematics, Technical University of Munich, Germany
Email address: carlos.amendola, mathias.drton, alex.grosdos, roser.homs@tum.de

Department of Mathematics, University of British Columbia, Canada
Email address: erobeva@ubc.ca

CÁLCULO DE ASÍNTOTAS GENERALIZADAS DE CURVAS ALGEBRAICAS

ELENA CAMPO-MONTALVO, MARIÁN FERNÁNDEZ DE SEVILLA, SONIA PÉREZ-DÍAZ

Resumen. Se presenta un algoritmo para calcular las *asíntotas generalizadas* o *g-asíntotas* de una curva algebraica plana, $\mathcal{C}$, definida implícitamente en $\mathbb{C}^2$. Las *g-asíntotas* generalizan el concepto clásico de asíntota de una curva definida por un polinomio de la forma $yg(x) - f(x)$. Para ello, se definen los conceptos de ramas infinitas y ramas convergentes, y se establecen los fundamentos a partir de los cuales se definirán las *g-asíntotas*, es decir, las curvas aproximantes y las curvas perfectas. Estos conceptos constituyen una herramienta fundamental para analizar el comportamiento de una curva en el infinito.

Introducción

En este trabajo se presenta una solución algorítmica que permite determinar el comportamiento en el infinito de una curva algebraica plana, $\mathcal{C}$, mediante el cálculo de las *asíntotas generalizadas*, o *g-asíntotas*, de sus ramas en puntos con coordenadas suficientemente grandes. Este concepto, generaliza el concepto clásico de asíntota y sus métodos de cálculo (véase p.e. [1, 2]).

De manera intuitiva, dada una curva $\mathcal{C}$, se dice que $\widetilde{\mathcal{C}}$ es una *g-asíntota* de $\mathcal{C}$, si $\widetilde{\mathcal{C}}$ es una curva del menor grado posible que aproxima a $\mathcal{C}$ en el infinito (véase [3, 4]).

El algoritmo que se presenta en la Sección 3, se sustenta sobre los estudios preliminares de la Sección 1, así como en los conceptos de *curva perfecta* y *g-asíntota* definidos en la Sección 2. Además, en la Sección 3 se presenta el algoritmo y un ejemplo que ilustra el método que se desarrolla en este trabajo.

Además, señalar que las novedades respecto los trabajos previos se basan en una mejora e implementación de los resultados que aquí se exponen, ilustrándolos mediante un algoritmo cuya complejidad se reduce al cálculo de una serie de Puiseux.

1. Preliminares y notación

En esta sección se introducen los conceptos de *ramas infinitas*, *ramas convergentes* y *curvas aproximantes*, derivados de investigaciones previas (ver [3, 4, 5, 6]).

Sea una curva algebraica plana irreducible, $\mathcal{C}$, definida en el espacio afín por un polinomio irreducible $f(x, y) \in \mathbb{R}[x, y]$ en el cuerpo $\mathbb{C}$. Debido a las implicaciones prácticas, se asume que la curva es real y, por ello, el polinomio implícito viene definido sobre $\mathbb{R}$. Sea $\mathcal{C}^* \subset \mathbb{P}^2(\mathbb{C})$ su correspondiente curva proyectiva definida por el polinomio homogéneo $F(x, y, z) = f_d(x, y) + zf_{d-1}(x, y) + z^2 f_{d-2}(x, y) + \ldots + z^d f_0(x, y) \in \mathbb{R}[x, y, z]$, con

Date: 12/02/2022.

La tercera autora ha sido parcialmente financiada por el proyecto del Ministerio de Ciencia e Innovación PID2020-113192GB-I00 (Visualización Matemática: Fundamentos, Algoritmos y Aplicaciones).

La ponencia en el Encuentro EACA 2022 ha sido presentada por la primera autora.

$d := \text{grado}(\mathcal{C})$, y sean los puntos de infinito de $\mathcal{C}^*$ de la forma $(1 : m : 0), m \in \mathbb{C}$ (en caso de existir el punto de infinito $(0 : 1 : 0)$, se aplica un cambio lineal de coordenadas).

En estas condiciones, a partir de la curva definida por el polinomio $g(y, z) = F(1 : y : z)$ y calculando las series de Puiseux, φ_i, $i = 1 \dots \text{grado}_y(g)$ de $g(y, z) = 0$ alrededor de $z = 0$, se obtienen las *ramas* de $\mathcal{C}$ (véase [4]). En lo que sigue denotamos como $\varphi(t) = m + a_1 t^{N_1/N} + a_2 t^{N_2/N} + a_3 t^{N_3/N} + \cdots$, $\quad a_i \neq 0, \forall i \in \mathbb{N}$, con $N_i \in \mathbb{N}$, $i = 1, \ldots$, y $0 < N_1 < N_2 < \cdots$ a una de estas series. Por tanto $g(\varphi(t), t) = 0$ en un entorno de $t = 0$ donde $\varphi(t)$ converge.

Definición 1.1. Se denomina *rama infinita* de la curva plana afín $\mathcal{C}$, en el punto de infinito $P = (1 : m : 0)$, $m \in \mathbb{C}$, al conjunto $B = \{(z, r(z)) \in \mathbb{C}^2 : z \in \mathbb{C}, |z| > M\}$, donde $r(z) = z\varphi(z^{-1}) = mz + a_1 z^{1-N_1/N} + a_2 z^{1-N_2/N} + a_3 z^{1-N_3/N} + \cdots$ y M es un cierto número natural.

Definición 1.2. Dadas dos *ramas*, $B = \{(z, r(z)) \in \mathbb{C}^2 : z \in \mathbb{C}, |z| > M\}$ y $\overline{B} = \{(z, \overline{r}(z)) \in \mathbb{C}^2 : z \in \mathbb{C}, |z| > \overline{M}\}$, se dice que son *convergentes* si $\lim_{z\to\infty}(\overline{r}(z) - r(z)) = 0$.

Definición 1.3. Sea una curva algebraica plana $\mathcal{C}$ con una rama infinita B. Se dice que una curva $\mathcal{D}$ se *aproxima* a $\mathcal{C}$ en su rama infinita B, si $\lim_{z\to\infty} d((z, r(z)), \mathcal{D}) = 0$ ($d(p, \mathcal{D}) = \min\{d(p, q) : q \in \mathcal{D}\}$).

En [4] se demuestra que si $\mathcal{C}$ es una curva plana con una rama infinita B entonces, una curva plana $\overline{\mathcal{C}}$ aproxima a $\mathcal{C}$ en B si y sólo si $\overline{\mathcal{C}}$ tiene una rama infinita $\overline{B}$ tal que B y $\overline{B}$ son convergentes.

2. Asíntotas generalizadas y curvas perfectas

A partir de los conceptos introducidos en la Sección 1, se obtienen las siguientes definiciones (véase [3]).

Definición 2.1. Una curva de grado d es una *curva perfecta* si no puede ser aproximada por ninguna curva de grado menor que d.

Obsérvese que una curva $\mathcal{C}$ que no sea perfecta puede aproximarse por otras curvas de menor grado.

Definición 2.2. Sea una curva algebraica plana $\mathcal{C}$ con una rama infinita B. Una curva, $\widetilde{\mathcal{C}}$, es una *g-asíntota* o *asíntota generalizada* de $\mathcal{C}$ en B, si es una curva perfecta que aproxima a $\mathcal{C}$ en B (en lo sucesivo se utilizará el término asíntota para referirse a estas).

Sea $\mathcal{C}$ con una rama $B = \{(z, r(z)) \in \mathbb{C}^2 : z \in \mathbb{C}, |z| > M\}$, donde $r(z) = mz + a_1 z^{1-N_1/N} + \cdots + a_k z^{1-N_k/N} + a_{k+1} z^{1-N_{k+1}/N} + \cdots$, con $a_1, a_2, \ldots \in \mathbb{C} \setminus \{0\}, m \in \mathbb{C}$, $N, N_1, N_2 \ldots \in \mathbb{N}$, y $0 < N_1 < N_2 < \cdots$. Supongamos que $N_k \leq N < N_{k+1}$, i.e. los términos $a_j z^{1-N_j/N}$ con $j \geq k + 1$ tienen exponente negativo. En lo que sigue, escribimos

$$r(z) = mz + a_1 z^{1-n_1/n} + \cdots + a_k z^{1-n_k/n} + a_{k+1} z^{1-N_{k+1}/N} + \cdots$$

con $\text{mcd}(N, N_1, \ldots, N_k) = b, N_j = n_j b, N = nb,\ j = 1, \ldots, k$. Es decir, simplificamos los exponentes tal que $\text{mcd}(n, n_1, \ldots, n_k) = 1$. Nótese que $0 < n_1 < n_2 < \cdots$, $n_k \leq n$, y $N < n_{k+1}$, i.e. los términos $a_j z^{1-N_j/N}$ con $j \geq k + 1$ tienen exponentes negativos. Sea

$\widetilde{r}(z) = mz + a_1 z^{1-n_1/n} + \cdots + a_k z^{1-n_k/n}$ los términos con exponente no negativo de $r(z)$. Aplicando el cambio $z = t^n$, se obtiene la parametrización propia de una curva $\widetilde{\mathcal{C}}$

$$\widetilde{\mathcal{P}}(t) = (t^n, mt^n + a_1 t^{n-n_1} + \cdots + a_k t^{n-n_k}) \in \mathbb{C}[t]^2,$$

donde $n, n_1, \ldots, n_k \in \mathbb{N}$, $\mathrm{mcd}(n, n_1, \ldots, n_k) = 1$, y $0 < n_1 < \cdots < n_k$, que es una asíntota de $\mathcal{C}$ (véase [3]).

3. Algoritmo para calcular asíntotas de curvas definidas implícitamente

El siguiente algoritmo calcula las parametrizaciones de las asíntotas de las ramas infinitas de la curva $\mathcal{C}$. Además, se ilustra el algoritmo con un ejemplo.

Data: $\mathcal{C}$, curva algebraica plana irreducible definida por $f(x, y) \in \mathbb{R}[x, y]$
Result: Asíntotas de $\mathcal{C}$
begin
  $F(x, y, z) \leftarrow CurvaProyectiva(\mathcal{C})$
  $P_1, \ldots, P_n \leftarrow PuntosdeInfinito(F(x, y, 0))$
  $g(y, z) \leftarrow F(1, y, z)$
  $\phi_1, \ldots, \phi_m \leftarrow RaícesdePuiseux(g(y, 0))$
  foreach ϕ_i de P_i **do**
    $r_i(z) \leftarrow z\phi_i(z^{-1})$, $B_i \leftarrow \{(z, r_i(z)) \in \mathbb{C}^2 : z \in \mathbb{C}, |z| > M_i\}$ /* Def. 1.1 */
    $\widetilde{r}_i(z) \leftarrow m_i z + a_{1,i} z^{1-n_{1,i}/n_i} + \cdots + a_{k_i,j} z^{1-n_{k_i,i}/n_i}$ /* Def. 2.2 */
    $\widetilde{\mathcal{P}}_i(t) \leftarrow (t^{n_i}, \tilde{r}_i(t^{n_i})) \in \mathbb{C}[t]^2$
  end
  return $\widetilde{\mathcal{C}}_i \leftarrow \widetilde{\mathcal{P}}_i(t)$, $i = 1, \ldots, n$
end

Para calcular las series de Puiseux puede utilizarse el paquete algcurves incluido en el sistema informático de álgebra Maple. También cabe señalar que el algoritmo anterior se ha implementado en Maple. Como se ha comentado anteriormente la complejidad del algoritmo depende de la complejidad de la expansión en series de Puiseux (véase [7]).

Ejemplo 3.1. Sea una curva $\mathcal{C}$, de grado $d = 6$, definida por el polinomio irreducible $f(x, y) = y^6 + 2y^5x + 3x^2 + 4xy \in \mathbb{R}[x, y]$. Como $f_6(x, y) = y^6 + 2y^5x$, se tiene que los puntos de infinito son $P_1 = (1 : 0 : 0)$ y $P_2 = (1 : -2 : 0)$.

1. Sea $P_1 = (1 : 0 : 0)$
   Iteración 1: Se tiene la rama infinita, $B_1 = \{(z, r_1(z)) \in \mathbb{C}^2 : z \in \mathbb{C}, |z| > M_1\}$ con
   $$r_1(z) = -\frac{48^{1/5}}{2} z - \frac{-72^{1/5}}{12} z^{-3} + \frac{108^{1/5}}{18} z^{-7} - \frac{-162^{1/5}13}{432} z^{-11} + \ldots.$$
   a) $\tilde{r}_1(z) = -\dfrac{48^{1/5}}{2} z.$ b) $\widetilde{\mathcal{P}}_1(t) = (t^5, -\dfrac{48^{1/5}}{2} t).$
2. Sea $P_2 = (1 : -2 : 0)$
   Iteración 2: Se tiene la rama infinita, $B_2 = \{(z, r_2(z)) \in \mathbb{C}^2 : z \in \mathbb{C}, |z| > M_2\}$ con
   $$r_2(z) = -2z - \frac{5}{32} z^{-3} + \ldots.$$
   a) $\tilde{r}_2(z) = -2z.$ b) $\widetilde{\mathcal{P}}_2(t) = (t, -2t).$

En la Figura 1 se representa la curva $\mathcal{C}$ y sus asíntotas generalizadas $\widetilde{\mathcal{C}}_1$ y $\widetilde{\mathcal{C}}_2$, definidas por las parametrizaciones $\widetilde{\mathcal{P}}_1$ y $\widetilde{\mathcal{P}}_2$, respectivamente.

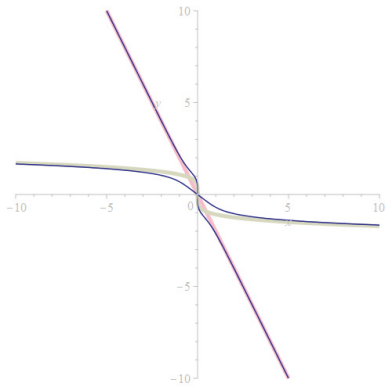


FIGURA 1. Asíntotas infinitas $\widetilde{\mathcal{C}}_1$ (beige) y $\widetilde{\mathcal{C}}_2$ (rosa) de la curva $\mathcal{C}$.

4. CONCLUSIONES

Las g-asíntotas determinan el comportamiento de una curva en el infinito. Con ellas, se pueden establecer modelos predictivos o de cálculo de tendencias, que mejoren los resultados de la regresión lineal simple. Además, como trabajo futuro, se plantea generalizar estos resultados a curvas definidas por una parametrización ([5, 6]), así como para superficies y estudiar las familias de asíntotas existentes.

REFERENCIAS

1. E. A. Maxwell, *An Analytical Calculus* vol. 3, Cambridge University Press, New York, (1962).
2. G. Zeng, *Computing the asymptotes for a real plane algebraic curve*. J. Algebra, (2) **316** (2007), 680–705.
3. A. Blasco, S. Pérez-Díaz, *Asymptotes and Perfect Curves*. C. Aided. Geom. D., (2) **31** (2014), 81-96.
4. A. Blasco, S. Pérez-Díaz, *Asymptotic Behavior of an Implicit Algebraic Plane Curve*. Comput. Aided. Geom. D., (7-8) **31** (2014), 345-357.
5. E. Campo-Montalvo, M. Fernández de Sevilla, S. Pérez-Díaz, *Computing branches and asymptotes of curves defined by a not rational parametrization*. Enviado, (2022).
6. E. Campo-Montalvo, M. Fernández de Sevilla, S. Pérez-Díaz, *A simple formula for the computation of branches and asymptotes of curves and some applications*. Comput. Aided. Geom. Design. https://doi.org/10.1016/j.cagd.2022.102084. (2022).
7. A. Poteaux, M. Rybowicz *Complexity bounds for the rational Newton-Puiseux algorithm over finite fields*. AAECC **22** (2011), 187–217.

Universidad de Alcalá. Dept. de Automática. 28871 Alcalá de Henares, Spain
Email address: elena.campo@uah.es

Universidad de Alcalá. Dept. de Ciencias de la Computación. 28871 Alcalá de Henares, Spain
Email address: marian.fernandaz@uah.es

Universidad de Alcalá. Dept. de Física y Matemáticas. 28871 Alcalá de Henares, Spain
Email address: sonia.perez@uah.es

MULTIPLE (REAL) ROOTS THROUGH SUBRESULTANTS

JORGE CARAVANTES AND LAUREANO GONZALEZ–VEGA

ABSTRACT. By using subresultants we characterise when multiple roots of univariate polynomials can be described as rational functions of the coefficients of the considered polynomial and in such a case, we provide closed formulae for those functions.

INTRODUCTION

By using subresultants we characterise those univariate polynomials with multiple roots such that these roots can be described rationally in terms of the coefficients of the considered polynomial. Moreover we show how these rational functions can be computed and as a by–product, we obtain information about the real roots of the considered polynomial. This technique (for degree four) has been very useful when determining the intersection curve of two quadrics in [4]. This new approach will prove that the topology of quartic and quintic curves can be computed easily even if the curve is not in general position and enable characterisation of the type of the curve arising when intersecting two ellipsoids.

1. GCD AND REAL ROOT COUNTING THROUGH SUBRESULTANTS

Subresultants are the tool to use when determining the gcd of two univariate polynomials or the number of different real roots of an univariate polynomial involving parameters or algebraic numbers as coefficients.

Definition 1.1. Let $P(T) = \sum_{i=0}^{p} a_i T^i, Q(T) = \sum_{i=0}^{q} b_i T^i \in \mathbb{R}[T]$ with $p \geq q$ and $j = 0, \ldots, q-1$. Taking $\delta_k = (-1)^{k(k+1)/2}$, the j–th subresultant polynomial of P and Q is ([3]):

$$\mathbf{Sres}_j(P,Q) = (-1)^j \delta_{p-j-1} \begin{vmatrix} a_p & a_{p-1} & a_{p-2} & \dots & \dots & a_0 & & & & \\ & \ddots & \ddots & \ddots & & & \ddots & & & \\ & & a_p & a_{p-1} & a_{p-2} & \dots & \dots & a_0 & & \\ b_q & b_{q-1} & b_{q-2} & \dots & \dots & \dots & b_0 & & & \\ & \ddots & \ddots & \ddots & & & & \ddots & & \\ & & b_q & b_{q-1} & b_{q-2} & \dots & \dots & \dots & b_0 & \\ & & & & & 1 & -T & & & \\ & & & & & & \ddots & \ddots & & \\ & & & & & & & 1 & -T & \end{vmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\end{matrix}}\right\} q-j \\ \left.\vphantom{\begin{matrix}a\\a\\a\end{matrix}}\right\} p-j \\ \left.\vphantom{\begin{matrix}a\\a\\a\end{matrix}}\right\} j \end{matrix}$$

The j–th subresultant coefficient $\mathbf{sres}_j(P,Q)$ is the coefficient of T^j in $\mathbf{Sres}_j(P,Q)$.

Both authors have been partially supported by PID2020-113192GB-I00/AEI/10.13039/501100011033 from the Spanish State Research Agency (Ministerio de Ciencia e Innovación).

The talk at the EACA 2022 meeting was given by the second author.

There are many different ways of defining and computing subresultants (see [1, 3]). The use here of only one sequence for dealing with the gcd and the real root counting problems leads to the "unusual" introduction of the sign $(-1)^j\delta_{p-j-1}$ in the previous definition.

Subresultant coefficients, $\mathbf{sres}_j(P,Q)$, provide the gcd of P and Q since:

$$\mathbf{Sres}_i(P,Q)=\gcd(P,Q) \iff \mathbf{sres}_j(P,Q)=0\ \forall j<i, \mathbf{sres}_i(P,Q)\neq 0 \tag{1}$$

The subresultant sequence of P, $p=\deg(P)$, is the subresultant sequence for P and P': $\mathbf{Sres}_p(P)=P$, $\mathbf{Sres}_{p-1}(P)=P'$ and $\mathbf{Sres}_j(P)=\mathbf{Sres}_j(P,P')$ $(0\leq j<p-1)$. The j–th subresultant coefficient of P is $\mathbf{sres}_j(P)=\mathrm{coef}_j(\mathbf{Sres}_j(P))$. The number of different real roots of P depends on the signs of such coefficients, so for a list $\mathbb{I}\in(\mathbb{R}-\{0\})^i$, we define $\mathbf{V}(\mathbb{I})$ and $\mathbf{P}(\mathbb{I})$ as the numbers of sign variations and sign permanences respectively.

Definition 1.2.
Let $a_0\neq 0, a_1,\ldots,a_n$ be elements in $\mathbb{R}$ with the following distribution of zeros:

$$\mathbb{I}=\{a_0,...,a_{i_1},0^{k_1},a_{i_1+k_1+1},...,a_{i_2},0^{k_2},a_{i_2+k_2+1},...,a_{i_3},0,\ldots,0,a_{i_{t-1}+k_{t-1}+1},...,a_{i_t},0^{k_t}\},$$

where 0^k means "k zeros" and any written a_i is not 0. Denoting $i_0+k_0+1=0$, we define:

$$\mathbf{C}(\mathbb{I})=\sum_{s=1}^{t}\big(\mathbf{P}(\{a_{i_{s-1}+k_{s-1}+1},\ldots,a_{i_s}\})-\mathbf{V}(\{a_{i_{s-1}+k_{s-1}+1},\ldots,a_{i_s}\})\big)+\sum_{s=1}^{t-1}\varepsilon_{i_s}$$

where ε_{i_s} is equal to 0 if k_s is odd and $(-1)^{\frac{k_s}{2}}\mathrm{sign}\,(a_{i_s+k_s+1}/a_{i_s})$ otherwise.

We now show the relation between subresultants and the number of real roots (see [1]).

Theorem 1.3. *For $P\in\mathbb{R}[T]$, $\mathbf{C}(\{\mathbf{sres}_{\deg(P)}(P),\ldots,\mathbf{sres}_0(P)\})=\#\{\alpha\in\mathbb{R}\colon P(\alpha)=0\}$.*

Finally, we define $s_k(P)$ and $s_{k,j}(P)$ or, when clear, just s_k and $s_{k,j}$, by the equality:

$$\mathbf{Sres}_k(P)\stackrel{\mathrm{def}}{=}s_k(P)T^k+s_{k,k-1}(P)T^{k-1}+\ldots+s_{k,1}(P)T+s_{k,0}(P)\ .$$

2. Multiple real roots of univariate polynomials through subresultants

Here we introduce formulas describing the multiple roots of an univariate polynomial in terms of their coefficients. This will be always possible for degree ≤ 5 and in most cases for degrees 6 and 7. It will be also characterised when possible in the general case. Recently ([2]), the multiplicity structure of a univariate polynomial has been characterised in terms of its coefficients. The formulae here introduced may for example be used to describe de y-coordinates of the points on a critical line of a real algebraic plane curve defined implicitely when computing its topology (see [1]).

Cases $\deg(P)\in\{2,3\}$ are not considered here since they are very easy to deal with.

2.1. $\deg(\mathbf{P})=\mathbf{4}$.

If $a_4\neq 0$ then $P(T)=a_4T^4+...+a_1T+a_0$ factors, when there are multiple roots, in five possible ways:

(1) $P(T)=a_4(T-\beta)^4$ with $\beta\in\mathbb{R}$.
(2) $P(T)=a_4(T-\beta)^3(T-\gamma)$ with $\beta,\gamma\in\mathbb{R}$ and $\beta\neq\gamma$.
(3) $P(T)=a_4(T-\beta)^2(T-\gamma)^2$ with $\beta,\gamma\in\mathbb{R}$ and $\beta\neq\gamma$.
(4) $P(T)=a_4(T-\gamma)^2(T-\overline{\gamma})^2$ with $\gamma\in\mathbb{C}-\mathbb{R}$.
(5) $P(T)=a_4(T-\beta)^2(T-\gamma_1)(T-\gamma_2)$ with $\gamma_1\neq\gamma_2$ (if $\gamma_1\in\mathbb{C}-\mathbb{R}$ then $\gamma_2=\overline{\gamma_1}\in\mathbb{C}-\mathbb{R}$).

Polynomials s_i and $s_{i,j}$ characterise each possibility in the following way (see (1)):

(1) If $s_0 = s_1 = s_2 = 0$ then $P(T) = a_4(T-\beta)^4$ and $\beta = -s_{3,2}/3s_3 = -a_3/4a_4$.
(2) If $s_0 = s_1 = 0$, $s_2 \neq 0$, $s_{2,1}^2 - 4s_2s_{2,0} = 0$ then $P(T) = a_4(T-\beta)^3(T-\gamma)$ with $\beta \neq \gamma \in \mathbb{R}$ and $\beta = -s_{2,1}/(2s_2)$ and $\gamma = a_0/(a_4\beta^3)$ when $\beta \neq 0$. If $\beta = 0$ then $\gamma = a_3/a_4$ with $a_3 \neq 0$.
(3) If $s_0 = s_1 = 0$, $s_2 \neq 0$, $s_{2,1}^2 - 4s_2s_{2,0} > 0$ then $P(T) = a_4(T-\beta_1)^2(T-\beta_2)^2$ with $\beta_1, \beta_2 \in \mathbb{R}$ and $s_2(T-\beta_1)(T-\beta_2) = \mathbf{Sres}_2(P) = s_2T^2 + s_{2,1}T + s_{2,0}$.
(4) If $s_0 = s_1 = 0$, $s_2 \neq 0$, $s_{2,1}^2 - 4s_2s_{2,0} < 0$ then $P(T) = a_4(T-\gamma)^2(T-\overline{\gamma})^2$ with $\gamma \in \mathbb{C} - \mathbb{R}$ and $s_2(T-\gamma)(T-\overline{\gamma}) = \mathbf{Sres}_2(P) = s_2T^2 + s_{2,1}T + s_{2,0}$.
(5) If $s_0 = 0$ and $s_1 \neq 0$ then $P(T) = a_4(T-\beta)^2(T-\gamma_1)(T-\gamma_2)$ with $\gamma_1 \neq \gamma_2$ (if $\gamma_1 \in \mathbb{C} - \mathbb{R}$ then $\gamma_2 = \overline{\gamma} \in \mathbb{C} - \mathbb{R}$) and $\beta = -s_{1,0}/s_1$ and $(T-\gamma_1)(T-\gamma_2) = P(T)/(a_4(T-\beta)^2)$.

In all cases we have characterised the real roots, simple or multiple, of any degree 4 polynomial with multiple roots as explicit functions of the coefficients of P.

2.2. $\deg(\mathbf{P}) = \mathbf{5}$. If $a_5 \neq 0$ then $P(T) = a_5T^5 + ... + a_1T + a_0$ factors, when there are multiple roots, in nine possible ways. We only show how to proceed in the following cases:

(1) $P(T) = a_5(T-\beta)^4(T-\gamma)$ with $\beta, \gamma \in \mathbb{R}$.
(2) $P(T) = a_5(T-\beta)^3(T-\gamma_1)(T-\gamma_2)$ with $\beta, \gamma_1, \gamma_2 \in \mathbb{R}$ and $\gamma_1 \neq \gamma_2$.

We define $\tau_0(T) = P(T)$ and, for $k \geq 1$, $\tau_k(T) = \gcd(\tau_{k-1}, \tau'_{k-1})$. Polynomials $s_i(P)$ will characterise each possibility for $\gcd(P, P') = \tau_1(P)$ (see (1)). We only consider two cases here (the remaining seven cases follow in a similar way):

(1) If $s_0(P) = s_1(P) = s_2(P) = 0$ and $s_3(P) \neq 0$ then $\tau_1(T) = \mathbf{Sres}_3(P)$. Two cases arise: $P(T) = a_5(T-\beta)^4(T-\gamma)$ or $P(T) = a_5(T-\beta)^3(T-\gamma)^2$ with $\beta \neq \gamma \in \mathbb{R}$.
(2) If $s_0(P) = 0$, $s_1(P) \neq 0$ then $\tau_1(T) = \mathbf{Sres}_1(P)$. The only possible cases are:
   (a) $P(T) = a_5(T-\beta)^2(T-\gamma_1)(T-\gamma_2)(T-\gamma_3)$ with $\beta \neq \gamma_1 \neq \gamma_2 \neq \gamma_3 \in \mathbb{R}$.
   (b) $P(T) = a_5(T-\beta)^2(T-\gamma_1)(T-\gamma_2)(T-\overline{\gamma_2})$ with $\beta \neq \gamma_1 \in \mathbb{R}$ and $\gamma_2 \in \mathbb{C} - \mathbb{R}$.

In order to separate the cases when $\deg(\tau_1(T)) = 3$ we note that $\tau_1(T) = \mathbf{Sres}_3(\tau_0)$. In the first case we have $\tau_1(T) = s_3(\tau_0)(T-\beta)^3$ and in the second one we have $\tau_1(T) = s_3(\tau_0)(T-\beta)^2(T-\gamma)$. $s_0(\tau_1)$ and $s_1(\tau_1)$ will separate these two cases:

- if $s_0(\tau_1) = s_1(\tau_1) = 0$ then $\tau_1(T) = s_3(\tau_0)(T-\beta)^3$ and $P(T) = a_5(T-\beta)^4(T-\gamma)$.
- if $s_0(\tau_1) = 0$, $s_1(\tau_1) \neq 0$ then $\tau_1(T) = s_3(\tau_0)(T-\beta)^2(T-\gamma)$ and $P(T) = a_5(T-\beta)^3(T-\gamma)^2$.

In the first case we have $\beta = -s_{3,2}(P)/(3s_3(P))$ and $\gamma = -a_0/(a_5\beta^4)$. And in the second one, we have $\tau_2(T) = \mathbf{Sres}_1(\tau_1) = s_1(\tau_1)(T-\beta)$, $\beta = -s_{1,1}(\tau_1)/s_1(\tau_1)$ and $\gamma = -s_{3,0}(P)/(s_3(P)\beta^2)$.

In both cases, 2(a) and 2(b), we have $\beta = -s_{1,1}(P)/s_1(P)$ and they are separated by analysing the signs of a_5, $s_3(P)$, $s_2(P)$ and $s_1(P)$:

- Case 2(a): $\mathbf{C}(\{a_5, 5a_5, s_3(P), s_2(P), s_1(P), 0\}) = 4$.
- Case 2(b): $\mathbf{C}(\{a_5, 5a_5, s_3(P), s_2(P), s_1(P), 0\}) = 2$.

In case 2(a) we have $(T-\gamma_1)(T-\gamma_2)(T-\gamma_3) = P(T)/(a_5(T-\beta)^2)$ and in case 2(b) we have $(T-\gamma_1)(T-\gamma_2)(T-\overline{\gamma_2}) = P(T)/(a_5(T-\beta)^2)$. Both polynomials have no multiple roots, and we know that they have exactly three and one different real roots respectively.

We have characterised the multiple real roots of any degree 5 polynomial with multiple roots as explicit functions of its coefficients. Simple real roots of these polynomials are also characterised in the same way (but cases 2(a) and 2(b) require a cubic squarefree equation).

2.3. **The general case.** When the degree of P is 6 or 7, we cannot proceed as before in all cases. The unique cases where the previous strategy fails are the following:

- $P(T) = a_6(T-\gamma_1)^2(T-\gamma_2)^2(T-\gamma_3)^2$ with $\gamma_1 \neq \gamma_2 \neq \gamma_3 \in \mathbb{R}$.
- $P(T) = a_6(T-\gamma_1)^2(T-\gamma_2)^2(T-\overline{\gamma_2})^2$ with $\gamma_1 \in \mathbb{R}$ and $\gamma_2 \in \mathbb{C}-\mathbb{R}$.
- $P(T) = a_7(T-\gamma_1)^2(T-\gamma_2)^2(T-\gamma_3)^2(T-\gamma_4)$ with $\gamma_1 \neq \gamma_2 \neq \gamma_3 \neq \gamma_4 \in \mathbb{R}$.
- $P(T) = a_7(T-\gamma_1)^2(T-\gamma_2)(T-\gamma_3)^2(T-\overline{\gamma_3})^2$ with $\gamma_1 \neq \gamma_2 \in \mathbb{R}$ and $\gamma_3 \in \mathbb{C}-\mathbb{R}$.

In all the remaining cases we can proceed as before concerning multiple real roots. In all cases we can compute a squarefree polynomial whose real roots are the simple real roots of the considered polynomial. The analysis above can be generalised as follows.

Theorem 2.1. *Let $P(T)$ be a polynomial in $\mathbb{R}[T]$ factorizing in the following way:*

$$P(T) = \prod_{i=1}^{r}(T-\beta_i)^{m_i} \prod_{i=r+1}^{r+s}((T-\gamma_i)(T-\overline{\gamma_i}))^{m_i} \prod_{k=1}^{t}(T-\delta_k) \prod_{k=t+1}^{t+q}(T-\phi_k)(T-\overline{\phi_k}) = \sum_{\ell=0}^{n} a_\ell T^\ell$$

with $m_i > 1$ and $\beta_i, \delta_k \in \mathbb{R}$ and $\gamma_i, \phi_k \in \mathbb{C}-\mathbb{R}$ (all of them different). Then:

(1) *If there are no repetitions in $m_1, m_2, \ldots, m_{r+s}$ then every β_i can be described explicitely like a rational function of the a_ℓ's.*
(2) *If the repeated elements in $m_1, m_2, \ldots, m_r$ appear at most twice and every m_i, $1 \leq i \leq r$, does not appear in $m_{r+1}, m_{r+2}, \ldots, m_{r+s}$ then every β_i can be described explicitely like a rational function of the a_ℓ's involving in some cases the square root of a polynomial in the a_ℓ's known to be strictly positive.*

The hypotheses in Theorem 2.1 are equivalent to, with the squarefree decomposition $P = P_1^1 ... P_k^k$, imposing, $\deg(P_i) \in \{0,1,2\}$, with P_i irreducible when quadratic, for all $i \geq 2$.

Proving this theorem is easy, using the squarefree decomposition of $P(T)$. Our proof provides the algorithm producing the desired description for the multiple real roots of $P(T)$ and the squarefree polynomial whose real roots are the simple real roots of $P(T)$.

References

[1] S. Basu, R. Pollack, M.-F. Roy: *Algorithms in Real Algebraic Geometry*. Algorithms and Computations in Mathematics **10**, Springer–Verlag, 2003.
[2] H. Hong, J. Yang: *A Condition for Multiplicity Structure of Univariate Polynomials*. J. Symb. Comput. **104**, 523–538, 2021.
[3] Y. B. Li: *A new approach for constructing subresultants*. Appl. Math. and Comp. **183**, 471–476, 2006.
[4] L. Gonzalez–Vega, A.Trocado: *Tools for analyzing the intersection curve between two quadrics through projection and lifting*. J. of Comp. and Appl. Math. **393**, 113522, 2021.

Universidad de Alcalá, Madrid, Spain
Email address: jorge.caravantes@uah.es

CUNEF Universidad, Madrid, Spain
Email address: laureano.gonzalez@cunef.edu

COMPUTING THE RELATIVE POSITION OF A PARABOLA AND AN ELLIPSE WITHOUT INTERSECTING THEM

JORGE CARAVANTES, GEMA M. DIAZ-TOCA, MARIO FIORAVANTI, AND LAUREANO GONZALEZ-VEGA

Abstract. Efficient methods to determine the relative position of two conics are of great interest for applications in robotics, computer animation, CAGD and other areas. We present a method to obtain the relative position of a parabola and an ellipse directly from the coefficients of their implicit equations, even if they are not given in canonical form, and avoiding the computation of the corresponding intersection points (and their characteristics).

Introduction

The problem of detecting the collisions or overlap of two conics in the plane is of interest for robotics, CAD/CAM, computer animation, etc., where conics are often used for modelling (or enclosing) the shape of the objects under consideration.

We present an efficient method to determine the relative position of a parabola $\mathcal{N}$ and an ellipse $\mathcal{M}$ in terms of the sign of several polynomial expressions derived from the coefficients of the implicit equations of $\mathcal{N}$ and $\mathcal{M}$. The main advantage of this approach relies on the fact that we do not have to compute the intersection points of $\mathcal{N}$ and $\mathcal{M}$ and their characteristics and it is especially useful when $\mathcal{N}$ and $\mathcal{M}$ depend on one or several parameters.

Here we follow an approach similar to the one presented in [3] and [5] but we reduce the number of sign conditions in some of the cases, and complete the proofs.

The problem considered here can be presented as a quantifier elimination problem over the reals (see [2]), since we are looking for conditions on the coefficients of the equations defining the considered conics in order they produce a prescribed geometric configuration. The bridge between the problem at hand and quantifier elimination is the characteristic equation of the two considered conics since the properties of its real roots determine each geometric configuration.

1. Characterising the relative position if $\mathcal{N}$ and $\mathcal{M}$ are in canonical form

There is an affine transformation that transforms the ellipse $\mathcal{M}$ in a circle of radius δ and such that $\mathcal{N}$ is in canonical form. Defining

$$\mathcal{X} = [x\ y\ 1], \quad N = \begin{bmatrix} a^{-2} & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{bmatrix}, \quad M = \begin{bmatrix} 1 & 0 & -x_c \\ 0 & 1 & -y_c \\ -x_c & -y_c & -\delta^2 + {x_c}^2 + {y_c}^2 \end{bmatrix}$$

The authors have been partially supported by the grant PID2020-113192GB-I00/AEI/10.13039/501100011033 (Mathematical Visualization: Foundations, Algorithms and Applications) from the Spanish State Research Agency (Ministerio de Ciencia e Innovación).

The talk at the EACA 2022 meeting was given by the third author.

we have that $\mathcal{N}$ is defined by $\mathcal{X}N\mathcal{X}^t = 0$ and $\mathcal{M}$ is defined by $\mathcal{X}M\mathcal{X}^t = 0$. The characteristic equation of N and M is $f(\lambda) = \det(\lambda N + M) = c_0\lambda^3 + c_1\lambda^2 + c_2\lambda + c_3$. Let Δ be the discriminant of $f(\lambda)$, and $g(\lambda) := f(\lambda - a^2) = c'_0\lambda^3 + c'_1\lambda^2 + c'_2\lambda + c'_3$.

The relative position of $\mathcal{N}$ and $\mathcal{M}$ when given in the canonical form previously presented in this section depends only on the roots of the characteristic equation of N and M as follows (see [5], Proposition 2.2).

Proposition 1.1.
Consider the parabola $\mathcal{N}$ and the circle $\mathcal{M}$, as above.

(1) *$\mathcal{M}$ and $\mathcal{N}$ are separated if and only if $f(\lambda) = 0$ has two distinct positive roots.*
(2) *$\mathcal{M}$ and $\mathcal{N}$ are externally tangent if and only if $f(\lambda) = 0$ has a positive double root.*
(3) *$\mathcal{M}$ is inside $\mathcal{N}$ if and only if $f(\lambda) = 0$ has three distinct negative roots, two of which are not less than $-a^2$ and one root belongs to $(-\infty, -a^2)$, or three roots are $-a^2, -a^2, -\delta^2/a^2$ when $a^2 > \delta$.*
(4) *$\mathcal{M}$ and $\mathcal{N}$ have only two intersection points if and only if $f(\lambda) = 0$ has two imaginary roots.*
(5) *$\mathcal{M}$ and $\mathcal{N}$ have four points of intersection if and only if $f(\lambda) = 0$ has three distinct negative roots which are not greater than $-a^2$.*
(6) *$\mathcal{M}$ and $\mathcal{N}$ have two points of intersection and an inner tangent point if and only if $f(\lambda) = 0$ has a negative double root and three roots are not greater than $-a^2$, where $a^2 \leq \delta$.*
(7) *$\mathcal{M}$ and $\mathcal{N}$ only have an inner tangent point, where $a^2 \neq \delta$ if and only if $f(\lambda) = 0$ has a negative double root which is greater than $-a^2$.*
(8) *$\mathcal{M}$ and $\mathcal{N}$ have two inner tangent points if and only if the roots of $f(\lambda) = 0$ are $-a^2$,$-a^2$,$-\delta^2/a^2$ where $a^2 < \delta$.*

This proposition is the reason why we say that we have reduced the problem at hand into a Quantifier Elimination problem, since finally we are looking for the conditions the c_i or c'_i must verify in order for the real roots of $f(\lambda)$ to have a prescribed behaviour. In this way, the next theorem reformulates the previous proposition in terms of the sign of Δ and the signs of the coefficients of $f(\lambda)$ and $g(\lambda)$, with the great advantage of not having to calculate the roots of the characteristic polynomial (see [3], section III).

Theorem 1.2.
Consider the parabola $\mathcal{N}$ and the circle $\mathcal{M}$, as above.

(1) *$\mathcal{M}$ and $\mathcal{N}$ are separated if and only if $\Delta > 0$, and $c_1 > 0$ or $c_2 > 0$.*
(2) *$\mathcal{M}$ and $\mathcal{N}$ are externally tangent if and only if $\Delta = 0$, and $c_1 > 0$ or $c_2 > 0$.*
(3) *$\mathcal{M}$ is inside $\mathcal{N}$ if and only if $\Delta > 0$, and $c_1 < 0$, $c_2 < 0$, and the number of sign changes in $-c_0$, c'_1, $-c'_2$, c'_3 is 0 or 1; or $c'_3 = 0$, $c'_2 = 0$, $a^2 > \delta$.*
(4) *$\mathcal{M}$ and $\mathcal{N}$ have only two intersection points if and only if $\Delta < 0$.*
(5) *$\mathcal{M}$ and $\mathcal{N}$ have four points of intersection if and only if $\Delta > 0, c'_2 < 0, c'_1 < 0$.*
(6) *$\mathcal{M}$ and $\mathcal{N}$ have two points of intersection and an inner tangent point if and only if $a^2 \leq \delta$, $\Delta = 0$, $c'_2 < 0, c'_1 < 0$.*
(7) *$\mathcal{M}$ and $\mathcal{N}$ have only an inner tangent point if and only if $a^2 \neq \delta$, $\Delta = 0$, $c_1 < 0, c_2 < 0$, and either $c'_3 < 0$, and $c'_2 > 0$ or $c'_1 > 0$ or $c'_3 = 0$, $c'_1 > 0$, $c'_2 < 0$.*
(8) *$\mathcal{M}$ and $\mathcal{N}$ have two inner tangent points if and only if $a^2 < \delta$, $c'_3 = 0$, and $c'_2 = 0$.*

2. Characterising the relative position of $\mathcal{N}$ and $\mathcal{M}$ in the general case

Now assume that the ellipse $\mathcal{M}$ and the parabola $\mathcal{N}$ are defined, respectively, by the symmetric matrices (not in canonical form)

$$\mathbf{M} = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{12} & a_{22} & a_{23} \\ a_{13} & a_{23} & a_{33} \end{pmatrix}, \quad \mathbf{N} = \begin{pmatrix} b_{11} & b_{12} & b_{13} \\ b_{12} & b_{22} & b_{23} \\ b_{13} & b_{23} & b_{33} \end{pmatrix},$$

We aim to characterize their relative position directly from their characteristic equation, as in [3], Section IV, although our results are different from the results in [3].

Let $L_3 := \det(\mathbf{M})$, $L_0 = \det \mathbf{N}$,

$$\mathbf{M_2} := \begin{pmatrix} a_{11} & a_{12} \\ a_{12} & a_{22} \end{pmatrix}, \quad T_1 := \det \mathbf{M_2}, \quad \mathbf{N_2} = \begin{pmatrix} b_{11} & b_{12} \\ b_{12} & b_{22} \end{pmatrix}.$$

Since $\mathcal{M}$ is a real ellipse, $T_1 > 0$ and $(a_{11} + a_{22})L_3 < 0$. Since $\mathcal{N}$ is a parabola, $\det \mathbf{N}_2 = 0$. Assume that $a_{11} > 0, a_{22} > 0, L_3 < 0, L_0 < 0$, and the interior of the ellipse $\mathcal{M}$ is defined by $\mathcal{X}M\mathcal{X}^T < 0$.

Let $L_1 := L_0 \text{Trace}(\mathbf{N}^{-1}\mathbf{M})$, $L_2 := L_3 \text{Trace}(\mathbf{M}^{-1}\mathbf{N})$ and $T := T_1 \text{Trace}(\mathbf{M_2}^{-1}\mathbf{N_2})$. Then, the characteristic polynomial of $\mathcal{M}$ and $\mathcal{N}$ is

$$F(\lambda) = \det(\lambda\mathbf{N} + \mathbf{M}) = L_0\lambda^3 + L_1\lambda^2 + L_2\lambda + L_3,$$

and its discriminant is $\Delta = -27L_0^2L_3^2 + 18L_0L_1L_2L_3 + L_1^2L_2^2 - 4L_1^3L_3 - 4L_0L_2^3$.

Let $\mathcal{S}_1$ be an affine transformation which transforms the given ellipse and parabola into

$$\mathcal{M}_1 : (x - x_c)^2 + (y - y_c)^2 = -L_3/T_1,$$

$$\mathcal{N}_1 : d_{11}x^2 + d_{22}y^2 + 2d_{12}xy + 2d_{13}x + 2d_{23}y + d_{33} = 0.$$

Let $\mathbf{A}$ be the matrix which defines the transformation $\mathcal{S}_1$, and let $\mathbf{M_1}$ and $\mathbf{N_1}$ be the matrices that define $\mathcal{M}_1$ and $\mathcal{N}_1$, respectively. Then, the characteristic equation is

$$F(\lambda) = (\det \mathbf{A})^{\mathbf{2}} \det(\lambda\mathbf{N_1} + \mathbf{M_1}).$$

Next, there is another affine transformation $\mathcal{S}_2$ which transforms $\mathcal{M}_1$ and $\mathcal{N}_1$, respectively into

$$\mathcal{M}_2 : (x' - x'_c) + (y' - y'_c)^2 = -L_3/T_1,$$

$$\mathcal{N}_2 : E_1x'^2 - 2E_2y' = 0,$$

with $E_1 = d_{11} + d_{22} = T/T_1$, $\quad E_2 = \sqrt{-L_0}/\sqrt{T}$.

Dividing the equation of $\mathcal{N}_2$ by E_2 we obtain the same form as in section 1, with $a^2 = E_2/E_1$. Thus,

$$f(\lambda) = \det\left(\lambda\hat{\mathbf{N}}_{\mathbf{2}}/E_2 + \hat{\mathbf{M}}_{\mathbf{2}}\right) = c_0\lambda^3 + c_1\lambda^2 + c_2\lambda + c_3,$$

with $c_0 = (\det \mathbf{A})^{-2}L_0/E_2^3$, $c_1 = (\det \mathbf{A})^{-2}L_1/E_2^2$, $c_2 = (\det \mathbf{A})^{-2}L_2/E_2$ and $c_3 = (\det \mathbf{A})^{-2}L_3$. Note that in order to apply Theorem 1.2, we have $\text{sign}(c_i) = \text{sign}(L_i)$ $(i = 0, \ldots, 3)$.

The coefficients of $G(\lambda) = F(\lambda - a^2) = c'_0\lambda^3 + c'_1\lambda^2 + c'_2\lambda + c'_3$ will be

$$c'_0 = -1/a^2, \quad c'_1 = (\det \mathbf{A})^{-2}(-3L_0a^2/E_2^3 + L_1/E_2^2),$$

$$c'_2 = (\det \mathbf{A})^{-2}(3L_0a^4/E_2^3 - 2L_1a^2/E_2^2 + L_2/E_2),$$

$$c'_3 = (\det \mathbf{A})^{-2}(-L_0a^6/E_2^3 + L_1a^4/E_2^2 - L_2a^2/E_2 + L_3).$$

Since $T > 0$, $E_2 > 0$, $a^2 = E_2/E_1$ and $E_1 = T/T_1$, we infer that c_1' has the same sign as $I_5 := -3L_0T_1 + L_1T$, c_2' has the same sign as $I_4 := 3L_0T_1^2 - 2L_1TT_1 + L_2T^2$ and c_3' has the same sign as $I_3 := -L_0T_1^3 + L_1TT_1^2 - L_2T^2T_1 + L_3T^3$. Let $I_2 := -T_1^3L_0 + L_3T^3$. Hence we can conclude the following.

Theorem 2.1.
The relationship between the ellipse $\mathcal{M}$ and the parabola $\mathcal{N}$ are as follows:

(1) *$\mathcal{M}$ and $\mathcal{N}$ are separated if and only if $\Delta > 0$ and $(L_1 > 0$ or $L_2 > 0)$.*
(2) *$\mathcal{M}$ and $\mathcal{N}$ are externally tangent if and only if $\Delta = 0$ and $(L_1 > 0$ or $L_2 > 0)$.*
(3) *$\mathcal{M}$ and $\mathcal{N}$ have four points of intersection if and only if $\Delta > 0$, $I_4 < 0$ and $I_5 < 0$.*
(4) *$\mathcal{M}$ and $\mathcal{N}$ have two points of intersection if and only if $\Delta < 0$.*
(5) *$\mathcal{M}$ and $\mathcal{N}$ have only one interior point of tangency if and only if*
$\{I_2 \neq 0, \Delta = 0, L_1 < 0, L_2 < 0, I_3 < 0$ and $(I_4 > 0$ or $I_5 > 0)\}$,
or $\{\Delta = 0, L_1 < 0, L_2 < 0, I_3 = 0, I_5 > 0, I_4 < 0\}$,
or $\{\Delta = 0, L_1 < 0, L_2 < 0, I_3 = 0, I_5 = 0, I_4 = 0\}$.
(6) *$\mathcal{M}$ and $\mathcal{N}$ have two inner points of tangency points if and only if $\Delta = 0$, $I_3 = 0$, $I_4 = 0$ and $I_5 < 0$.*
(7) *$\mathcal{M}$ and $\mathcal{N}$ have one interior point of tangency and two points of intersection points if and only if $I_2 \leq 0, \Delta = 0, I_4 < 0, I_5 < 0$.*
(8) *$\mathcal{M}$ is inside $\mathcal{N}$ if and only if $\{\Delta > 0, L_1 < 0, L_2 < 0, I_4 > 0\}$ or $\{\Delta > 0, L_1 < 0, L_2 < 0, I_5 \geq 0, I_4 \leq 0, I_3 < 0\}$, or $\{I_3 = 0, I_4 = 0, I_5 > 0\}$.*

We recover here the same formulae introduced in [1, 4] for characterising when two ellipses are separated or they are externally tangent. This is not a surprise since the root pattern for these two geometric configurations is the same in the case we have considered here.

References

[1] M. Alberich-Carramiñana, B. Elizalde, F. Thomas: *New algebraic conditions for the identification of the relative position of two coplanar ellipses*. Computer Aided Geometric Design **54**, 35–48, 2017.
[2] S. Basu, R. Pollack, M.-F. Roy: *Algorithms in Real Algebraic Geometry*. Algorithms and Computations in Mathematics **10**, Springer–Verlag, 2003.
[3] M. Chen, X. Hou, X. Qiu: *An explicit criterion for the positional relationship of an ellipse and a parabola*. IEEE International Conference on Systems, Man and Cybernetics (SMC 2008), 825–829, 2008.
[4] J. Caravantes, G.M. Diaz–Toca, M. Fioravanti, L. Gonzalez–Vega: *Solving the interference problem for ellipses and ellipsoids: New formulae*. J. of Comp. and App. Math., **407**, 114072, 2022.
[5] Y. Liu, F. Chen: *Algebraic Conditions for Classifying the Positional Relationships Between Two Conics and Their Applications*. J. Comput. Sci. Technol., **19**, 665–673, 2004.

Universidad de Alcalá
E-mail address: jorge.caravantes@uah.es

Universidad de Murcia
E-mail address: gemadiaz@um.es

Universidad de Cantabria
E-mail address: mario.fioravanti@unican.es

CUNEF Universidad
E-mail address: laureano.gonzalez@cunef.edu

BOHEMIAN MATRICES: A SOURCE OF CHALLENGES

E. CHAN, R. CORLESS, L. GONZALEZ-VEGA, J. R. SENDRA, AND J. SENDRA

Abstract. A family of Bohemian matrices is a set of matrices where the entries are independently sampled from a finite set, usually of integers. Such families arise in many applications (e.g. compressed sensing) and the properties of matrices selected "at random" from such families are of practical and mathematical interest. Studying these matrices leads to many unanswered questions. In the abstract, we focus on two different problems: the study of some properties of a family of upper Hessenberg Toeplitz structured Bohemian matrices, and the analysis of generalized (inner) Bohemian inverses.

Introduction

A matrix is called **Bohemian** if its entries come from a fixed finite discrete (and hence bounded) set, usually of integers called the *population* P. We look at Bohemian matrices, and specifically those with entries from $P = \{-1, 0, +1\}$. The name is a mnemonic for **Bo**unded **He**ight **M**atrix of **I**ntegers. Such objects arise naturally in many applications. For instance, in signal processing, where they use Bernoulli matrices, or error correcting codes working with Hadamard matrices, etc. Other fields where they can be applied are combinatorics or graph theory, among others.

Bohemian families have been studied for a long time, although not under that name. For instance, Olga Taussky-Todd's paper "Matrices of Rational Integers" [19] begins by saying:

> "This subject is very vast and very old. It includes all of the arithmetic theory of quadratic forms, as well as many of other classical subjects, such as latin squares and matrices with elements $+1$ or -1 which enter into Euler's, Sylvester's or Hadamard's famous conjectures."

Taussky-Todd also discussed matrices with small integer entries in [20]. The paper [14], by C. W. Gear, is another instance. These families are interesting objects of study in themselves, and susceptible to brute-force computational experiments (both ideas are studied in [20]) as well as to asymptotic analysis. Such experiments have generated many conjectures, some of which are listed on the Characteristic Polynomial Database [21]. Matrices with a population $P = \{-1, 0, +1\}$ occur naturally as exemplars of "sign-pattern matrices", see [5] and [15]. For early theorems, see [16].

The inspiration of the authors in [10], [12],[13], and [22] for studying these types of problems originated when exploring density plots of the eigenvalues of such types of random matrices. See http://www.bohemianmatrices.com.

The authors were partially supported by the grant PID2020-113192GB-I00 (Mathematical Visualization: Foundations, Algorithms and Applications) from the Spanish MICINN.

The talk at the EACA 2022 meeting has been given by the fifth author.

Contents

The idea of visualizing the eigenvalues of random samples of matrices is not new. L. N. Trefethen [23], used this idea to visualize the pseudospectra of several test matrices. Related to the eigenvalues of matrices, many authors have studied the zeros of polynomials whose coefficients belong to discrete sets of integers. Early studies by Odlyzko and Poonen [18] focused on the zeros of polynomials with coefficients in $\{0, 1\}$. More recently, the distributions of the roots of Littlewood polynomials [17] have been studied in [1], [3], [4], and [11]. In Figure 1[1], we can visualize the Bohemian eigenvalues of a sample of 1 million 100×100 upper Hessenberg matrices with a Toeplitz structure. The entries are sampled from the population $\{-1, 1\}$, the entries on the main diagonal are fixed at 0, and entries on the subdiagonal are fixed at 1. See http://www.bohemianmatrices.com/gallery/.

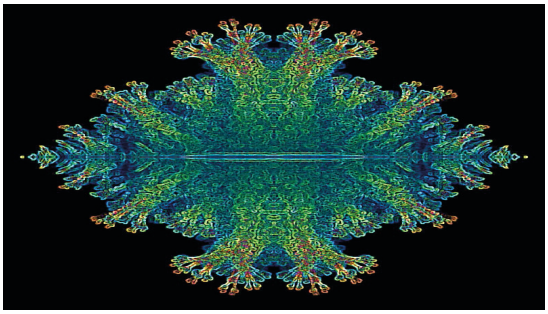


FIGURE 1. A density plot in the complex plane of the Bohemian eigenvalues of a sample of 1 million 100×100 upper Hessenberg Toeplitz matrices.

Specializing in Bohemian families with the same strong structure (e.g. upper Hessenberg, Toeplitz, circulant, etc.) has shown to be more successful in developing an understanding of relationships within these families. The study of eigenvalues of structured Bohemians (e.g. tridiagonal, complex symmetric) has recently been undertaken and several puzzling features result from extensive experimental computations. For instance, some of the images at http://www.bohemianmatrices.com/gallery show common features including "holes". These visible features of graphs of roots and eigenvalues from structured families of polynomials and matrices have been previously studied. One well-known set of polynomials whose roots produce interesting pictures are the Littlewood polynomials, $p(x) = \sum_{i=0}^{n} a_i x^i$, where $a_i \in \{-1, +1\}$. These polynomials have been studied in [1], [3], and [4]. Similarly, polynomials with coefficients $\{0, 1\}$ (also called Newman polynomials) have been studied by Odlyzko and Poonen [18].

1. MOTIVATION

To start with, the natural first question is: why Bohemian Matrices? The original motivation of the authors of [8] was to test problems for various algorithms. An overview of some of the original interest in Bohemian matrices can be found in [6], [7], [8] and [22]. An interesting challenge is to analyze the distribution of the eigenvalues for particular structured bohemains. These distributions turn out to be helpful for understanding some properties.

[1]Picture in Figure 1 has been taken, and is available at http://www.bohemianmatrices.com/gallery/.

This exploration has been inspired by many questions, most of which are computational. For instance, for a given dimension and population, the set of Bohemian matrices is finite, but:

: How many are singular?
: How many distinct characteristic polynomials does the family have? Which is the maximum height?
: How many distinct eigenvalues does the family contain? How many are real?
: Which eigenvalue has the highest density?
: How many distinct Jordan canonical forms are there?
: Characterize the set of non-singular Bohemian with inverse being Bohemian w.r.t. the same population.
: Characterize the set of Bohemians with generalized inverse being Bohemian w.r.t. the same population.
: What can we say about Sylvester matrices of polynomials with coefficients in the fixed population?
: .....

Answering these questions yields challenges and, in turn, provides new opportunities. However, difficulties quickly appear. For instance, the number of possible Bohemian matrices of dimension n is typically quadratically exponential ($\exp(cn^2)$ for some c), depending on the matrix structure.

2. Study of some Bohemian Problems

Taking a look at the tentative (certainly incomplete) list of questions mentioned above, one can broadly consider two types of problems. Some with a clearly computational flavor, even, enumerative, as for instance computing the number of singular bohemian matrices of a fixed order a population, and others of a more theoretical nature that focus on the existence of bohemian matrices after an algebraic manipulation, such as knowing which invertible bohemian matrices have bohemian inverses. In this talk, we will describe some of our results in two different problems, each belonging to each of these two focus.

On one hand, we study some properties of a family of upper Hessenberg Toeplitz structured Bohemian matrices. In this context, we analyze the characteristic polynomials and we obtain formulas on the "maximal characteristic polynomial height" for the matrices not only upper Hessenberg, but Toeplitz. We also give an answer to the question on which matrices reach the maximum characteristic height; these results appear in [8].

On the other, we analyze the structure of the set of Bohemian matrices, with a fixed population, and of some particular form, which generalized inner inverse is again Bohemian. This analysis has to be seen as a first step toward the characterization of Bohemian matrices with Moore-Penrose inverse being Bohemian too. The results presented in this second problem are taken from [9].

References

[1] J. Baez. The beauty of roots. https://johncarlosbaez.wordpress.com/2011/12/11/the-beauty-of-roots/, 2011.

[2] Beaucoup, Frank and Borwein, Peter and Boyd, David W and Pinner, Christopher, Multiple roots of $[-1,1]$ power series. Journal of the London Mathematical Society. volume 57, 1, pp. 135–147, 1998. Cambridge University Press.
[3] P. Borwein, L. Jorgenson, Visible structures in number theory, Am. Math. Mon. 108 (2001) 897–910.
[4] P. Borwein, C. Pinner, Polynomials with 0,+1,-1coefficients and a root close to a given point, Can. J. Math. 49 (1997) 887–915.
[5] C. Briat, Sign properties of Metzler matrices with applications, Linear Algebra Appl. 515 (2017) 53–86.
[6] E.Y.S. Chan, A comparison of solution methods for Mandelbrot-like polynomials, Electronic Thesis and Dissertation Repository, The University of Western Ontario, 2016, https://ir .lib .uwo .ca /etd /4028.
[7] E.Y.S. Chan, R.M. Corless, L. Gonzalez-Vega, J.R. Sendra, J. Sendra, Algebraic linearizations of matrix polynomials, Linear Algebra Appl. 563 (2019) 373–399.
[8] E.Y.S. Chan, R.M. Corless, L. Gonzalez-Vega, J.R. Sendra, J. Sendra, S. E. Thornton, Upper Hessenberg and Toeplitz Bohemians, Linear Algebra Appl. 601 (2020) 372–100.
[9] E.Y.S. Chan, R.M. Corless, L. Gonzalez-Vega, J.R. Sendra, J. Sendra, S. E. Thornton, Applied Mathematics and Computation Volume 421, 126945 (2022).
[10] R.M. Corless, Generalized companion matrices in the Lagrange basis, in: Proceedings EACA, Universidad de Cantabria, Santander, Spain, 2004, pp.317–322.
[11] D. Christensen. Plots of roots of polynomials with integer coefficients. http: //jdc.math.uwo.ca/roots/. Accessed: 2016-06-25.
[12] R.M. Corless, S. Thornton, Visualizing eigenvalues of random matrices, ACM Commun. Comput. Algebra 50 (2016) 35–39, https://doi .org /10 .1145 /2930964 .2930969.
[13] R.M. Corless, S.E. Thornton, The Bohemian eigenvalue project, ACM Commun. Comput. Algebra 50 (2016) 158–160.
[14] C. Gear, A simple set of test matrices for eigenvalue programs, Math. Comput. 23 (1969) 119–125.
[15] F.J. Hall, Z. Li, Sign pattern matrices, in: L. Hogben (Ed.), Handbook of Linear Algebra, Chapman and Hall/CRC, 2013 (ch. 42).
[16] C. Jeffries, V. Klee, P. Van den Driessche, When is a matrix sign stable?, Can. J. Math. 29 (1977) 315—326.
[17] J. E. Littlewood. On polynomials $\sum^n \pm z^m, \sum^n e^{\alpha_m i} z^m, z = e^{\theta i}$. Journal of the London Mathematical Society, 41:367–376,1966.
[18] A.M. Odlyzko, B. Ponnen, Zeros of polynomials with 0,1 coefficients, in: B. Salvy (Ed.), Algorithms Seminar, vol.2130, December 1993, pp.169–172.
[19] O. Taussky, Matrices of rational integers, Bull. Am. Math. Soc. 66 (1960) 327–345.
[20] O. Taussky, Some computational problems involving integral matrices, J. Res. Natl. Bur. Stand. B, Math. Sci. 65 (1961) 15–17.
[21] S.E. Thornton, The characteristic polynomial database, available at http://bohemianmatrices .com /cpdb, Sept. 7, 2018
[22] S. E. Thornton, Algorithms for Bohemian Matrices, Electronic Thesis and Dissertation Repository,The University of Western Ontario, 2019, https://ir.lib.uwo.ca/etd/6069/.
[23] L. N. Trefethen. Pseudospectra of matrices. Numerical analysis, 91:234–266, 1991.

1 School of Medicine, The Chinese University of Hong Kong, Shenzhen, China
Email address: eunicechan@cuhk.edu.cn

2 School of Mathematical and Statistical Sciences, Western University, Canada

3,5 CUNEF University. Department of Quantitative Methods. Madrid. Spain
Email address: laureano.gonzalez@cunef.edu
Email address: juana.sendra@cunef.edu

4 Universidad of Alcalá. Dpto. Física y Matemáticas. Spain
Email address: rafael.sendra@uah.es

A LAPLACIAN DECOMPOSITION ALGORITHM FOR SQUARE MATRICES

J. ALBERTO CONEJERO, ANTONIO FALCÓ, AND MARÍA MORA

Abstract. Many of today's problems can be posed as a system of equations with the form $A\mathbf{x} = \mathbf{b}$. When A has the form

$$A = \sum_{i=1}^{d} \mathrm{id}_{n_1} \otimes \ldots \mathrm{id}_{n_{i-1}} \otimes A_i \otimes \mathrm{id}_{n_{i+1}} \otimes \cdots \otimes \mathrm{id}_{n_d},$$

we say that A is a Laplacian matrix. For example, these matrices appear when discretizing some PDEs, such as the Poisson equation, and are an interesting object of study since the Proper Generalized Decomposition algorithm converges very quickly with the solution of the associated linear system.

This made us wonder if a generic square matrix $M \in \mathrm{GL}(\mathbb{R}^N)$ could be decomposed in some way so that the study of the associated linear problem $M\mathbf{x} = \mathbf{b}$ would be simpler. In the main theorem of this work, we present a decomposition of the space $\mathbb{R}^{N\times N}$ that will help us to determine the matrix decomposition we are looking for. In addition, we will show the procedure to be carried out for it in the form of an algorithm.

Introduction and Motivation

Linear systems are widely used to approach computational models in applied sciences, e.g. in mechanics after the discretization of a partial differential equation. There are numerous mechanisms to deal with this type of problem. However, most of them lose efficiency as the size of the matrices or vectors involved increases. This effect is known as the *curse of dimensionality problem*. To try to solve this drawback, we can use tensor-based algorithms [5], since their use significantly reduces the number of operations that we must employ [2].

One of the most popular techniques among the algorithms based on tensor products strategies [3] is the Proper Generalized Decomposition (PGD) family, based on the Greedy Rank-One Update (GROU) algorithm [4, 7]. We observe, from the study of this procedure to solve high-dimensional linear systems, that there is a type of matrices for which the algorithm works particularly well: very fast convergence and a very good approximation of the solution. These are Laplacian-Like matrices, which have the form

$$A = \sum_{i=1}^{d} \mathrm{id}_{[n_i]} \otimes A_i \doteq \sum_{i=1}^{d} \mathrm{id}_{n_1} \otimes \cdots \otimes \mathrm{id}_{n_{i-1}} \otimes A_i \otimes \mathrm{id}_{n_{i+1}} \otimes \cdots \otimes \mathrm{id}_{n_d},$$

and which can be easily related with the classical Laplacian operator [6].

The third author has been partially supported by the Government of the Valencian Community and the European Social Fund (grant number ACIF/2020/269).

The talk at the EACA 2022 meeting was given by the third author.

Contents

For example, this is the case with the famous Poisson equation $-\Delta\phi = \mathbf{f}$. Using derivative approximations and finite difference methods, we can write the Poisson equation in discrete form as a linear system $A \cdot \phi_{ijk} = -\mathbf{f}_{ijk}$, where A is a block matrix (details in [4]). In Figure 1, we compare the CPU time employed in solving this discrete Poisson problem, with A written in Laplacian form, when we solve the problem by using the Greedy Algorithm and by the Matlab operator $\mathbf{x} = A\backslash\mathbf{b}$, for different number of nodes in $(0,1)^3$.

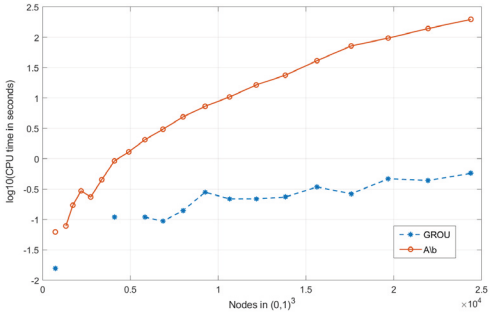


FIGURE 1. CPU-Time comparative

1. The Laplacian Decomposition. Main result

Suppose we have a linear system of the form $A\mathbf{x} = \mathbf{b}$, with A a square matrix in $\mathbb{R}^{N\times N}$. We want to approximate the matrix A by means of a matrix in Laplacian form $L_A \in \mathbb{R}^{N\times N}$, and solve the associated Laplacian linear system $L_A\mathbf{x} = \mathbf{b}$, in order to approximate the solution of the original system $\mathbf{x}^*$ by the solution obtained from the Laplacian system $\mathbf{x}_L^*$. To do this, we present the following result:

Theorem 1.1. *The set of Laplacian matrices $\mathcal{L}$ is a subspace of $\mathbb{R}^{N\times N}$ that contains the identity matrix, id_N. Moreover, if $N = n_1 \cdots n_d$, there is a linear subspace $\Delta \subset \mathcal{L}$,*

$$\Delta = \bigoplus_{i=1}^{d} \mathrm{span}\{\mathrm{id}_N\}^{\perp_i},$$

where $\mathrm{span}\{\mathrm{id}_N\}^{\perp_i}$ is the orthogonal complement of $\mathrm{span}\{\mathrm{id}_N\}$ in $\mathrm{span}\{\mathrm{id}_{n_i}\} \otimes \mathbb{R}^{n_i\times n_i}$ for $1 \le i \le d$, such that $\mathrm{id}_N \notin \Delta$.

Since $\mathbb{R}^{N\times N} = \Delta \oplus \Delta^{\perp}$, we can decompose any square matrix into its Laplacian approximation (which is computed by projecting onto Δ) and a linearly independent matrix to it. Furthermore, if we work with the Frobenius norm, $\mathrm{span}\{\mathrm{id}_N\}^{\perp_i} = \{\mathrm{id}_{[n_i]} \otimes A_i : \mathrm{tr}(A_i) = 0\}$, so $A \in \Delta$ iff

$$A = \sum_{i=1}^{d} \mathrm{id}_{[n_i]} \otimes A_i, \quad \text{with} \quad \mathrm{tr}(A_i) = 0,\ i = 1, \dots, d.$$

In order to be able to project in Δ and calculate the Laplacian decomposition of A, we need to calculate the A_i matrices in some way. Relying on the property that says that $\mathrm{tr}(ST) = 0$ if S and T are symmetric and skew-symmetric matrices respectively, we propose the following result:

Theorem 1.2. *Let $A \in \mathbb{R}^{N\times N}$ with $N = n_1 \cdots n_d$, and given d skew-symmetric matrices $B_i \in \mathbb{R}^{n_i \times n_i}$, $1 \leq i \leq d$, we can calculate one projection of A in $\Delta = \bigoplus_{i=1}^{d} \operatorname{span}\{\mathrm{id}_N\}^{\perp_i}$ as*

$$P_\Delta(A) = \sum_{i=1}^{d} \mathrm{id}_{n_1} \otimes \cdots \otimes \mathrm{id}_{n_{i-1}} \otimes \left(X_i + X_i^\top\right) B_i \otimes \mathrm{id}_{n_{i+1}} \otimes \cdots \otimes \mathrm{id}_{n_d},$$

where X_i are obtained by solving the successive minimization problems

$$\min_{X_i \in \mathbb{R}^{n_i \times n_i}} \left\| A - \sum_{i=1}^{d} \mathrm{id}_{[n_i]} \otimes \left(X_i + X_i^\top\right) B_i \right\|.$$

The proof of this result poses an iterative argument similar to the procedure of the Alternating Least Square (ALS) algorithm, where the error given by the norm of the residue is reduced by updating the terms that are part of the Laplacian decomposition. This procedure can be described by the following algorithm, given in pseudocode form:

Algorithm 1 Laplacian decomposition Algorithm

procedure LAP(A, `iter_max`, `tol`)
  choose $B_i \in \mathbb{R}^{n_i \times n_i}$ skew-symmetric matrices, for $i = 1, 2 \ldots, d$.
  `iter` $= 1$, `Lap` $= 0$
  while `iter` $<$ `iter_max` **do**
    $A \leftarrow A -$ `Lap`
    for $k = 1, 2, \ldots, d$ **do**
      $P_k(A) = \mathrm{id}_{n_1} \otimes \cdots \otimes \mathrm{id}_{n_{k-1}} \otimes (X_k + X_k^\top) B_k \otimes \mathrm{id}_{n_{k+1}} \otimes \cdots \otimes \mathrm{id}_{n_d}$
      $X_k \leftarrow \min_{X_k} \|A - \sum_{i=1}^{k} P_i(A)\|$
      `Lap` $=$ `Lap` $+ P_k(A)$
    end for
    if $\|A -$ `Lap`$\|_2 <$ `tol` **then goto** 15
    end if
    `iter` $=$ `iter` $+ 1$
  end while
  return `Lap`
end procedure

2. A numerical example

Let us consider the simple graph $G(V, E)$, with $V = \{1, 2, \ldots, 6\}$ the set of nodes and $E = \{(1,2), (1,4), (2,3), (2,5), (3,6), (4,5), (5,6)\}$ the set of edges. Then, the adjacency matrix of G is

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

We want to find a Laplacian decomposition of the matrix $A \in \mathbb{R}^{6\times 6}$ and for this, we need to set the basis on which to project. Since $n_1 = 2$, $n_2 = 3$, we choose for example the following

skew-symmetric matrices as the basis

$$B_1 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{and} \quad B_2 = \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}.$$

We then search for $X_1 \in \mathbb{R}^{2\times 2}$, $X_2 \in \mathbb{R}^{3\times 3}$ matrices so that

$$P_\Delta(A) = (X_1 + X_1^\top)B_1 \otimes \mathrm{id}_{n_2} + \mathrm{id}_{n_1} \otimes (X_2 + X_2^\top)B_2,$$

would be the best Laplacian approximation of the matrix A for the chosen parameterization. If we proceed according to the algorithm, that is, calculate X_i so that

$$\min_{X_i} \|A - \sum_{k=1}^{i} P_k(A)\|_F, \quad \text{where} \quad P_k(A) = \mathrm{id}_{[n_k]} \otimes (X_k + X_k^\top)B_k,$$

we obtain that

$$X_1 = \begin{pmatrix} 1/2 & 0 \\ 0 & -1/2 \end{pmatrix} \quad \text{and} \quad X_2 = \begin{pmatrix} 1/4 & 0 & 1/4 \\ 0 & -1/2 & 0 \\ 1/4 & 0 & 1/4 \end{pmatrix}.$$

To determine how good the Laplacian approximation obtained is, we calculate the value of the residue; since $||A - P_\Delta(A)|| = 0$, the matrix $A \in \Delta$, and we can write it as

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes \mathrm{id}_{n_2} + \mathrm{id}_{n_1} \otimes \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} = P_\Delta(A).$$

Finally, the "goodness" of the approximation depends on the basis chosen. For example, if we replace $b_{23} = 1$ and $b_{32} = -1$ in B_2, we cannot obtain an exact Laplacian decomposition of A.

References

[1] J. A. Conejero, A. Falcó and M. Mora. On the best approximation of square matrices in Laplacian-like form. *Preprint*, 2022.

[2] W. Hackbusch, Tensor Spaces and Numerical Tensor Calculus (Second Edition). Springer Series in Computational Mathematics 56, Springer-Verlag, Heidelberg, 2019.

[3] V. Simoncini, Numerical solution of a class of third order tensor linear equations. *Bollettino dell'Unione Matematica Italiana* 13:429–439, 2020.

[4] A. Ammar, F. Chinesta and A. Falcó, On the convergence of a Greedy Rank-One Update Algorithm for a class of Linear Systems. *Archives of Computational Methods in Engineering*, 17(4):473–486, 2010.

[5] A. Nouy, Low-Rank Methods for High-Dimensional Approximation and Model Order Reduction. *Model Reduction and Approximation*, 171–226, 2017.

[6] G. Heidel, V. Khoromskaia, B.N. Khoromskij and V. Schulz, Tensor product method for fast solution of optimal control problems with fractional multidimensional Laplacian in constraints, *Journal of Computational Physics*, 424:109865, 2021.

[7] I. Georgieva and C. Hofreither, Greedy low-rank approximation in Tucker format of solutions of tensor linear systems. *Journal of Computational and Applied Mathematics*, 358:206–220, 2019.

Universitat Politècnica de València, Camí de Vera, s/n, 46022, València
Email address: aconejero@upv.es

Universidad CEU Cardenal Herrera, Carrer Lluís Vives, 1, 46115, Alfara del Patriarca, Valencia
Email address: afalco@uchceu.es

Universitat Politècnica de València, Camí de Vera, s/n, 46022, València
Email address: mamoji7@posgrado.upv.es

JUMPING WALLS AND TOPOLOGICAL TYPE OF PLANE CURVES

FERRAN DACHS-CADEFAU

Abstract. In their respective PhD theses, Järvilehto (in [6]) and Tucker (in [9]) studied the relation between the jumping numbers of a curve and their equisingularity class. In this note we present how we can recover the equisingularity class of a tuple of analytically irreducible plane curves and the one of its product from its associated jumping walls, and show that in fact, we have enough information with the jumping numbers of each of the branches and those of the product of each pair.

Introduction

In this note we will consider a germ (X, O) of a smooth complex surface, the local ring $\mathcal{O}_{X,O}$ at O, and $\boldsymbol{f} = (f_1, \dots, f_r)$ will be a tuple of curves (at the moment, not necessarily analytically irreducible), define $C_i \equiv \{f_i = 0\}$. We will briefly recall some notations that can be found in more detail in [1] and [2].

Definition 0.1. A **log-resolution** of (X, D), with D a given divisor on X, is a proper birational map $\pi : X' \to X$ such that X' is smooth; and the divisor $\pi^*D + Exc(\pi)$ has simple normal crossings.

Associated with the log-resolution, we have the relative canonical divisor K_π, which is defined as follows $K_\pi = K_{X'} - \pi^*(K_X) = \sum_{i=1}^s k_i E_i \in Div(X')$ where $K_{X'}$ and K_X are canonical divisors of X' and X respectively, and E_i, with $i = 1, \dots, s$ are the exceptional and non-exceptional divisors[1]. The relative canonical divisor can be computed using the adjunction formula.

The main objects we are interested in are the mixed multiplier ideals.

Definition 0.2. Let $\boldsymbol{f} := (f_1, \dots, f_r)$ be a tuple of curves, define $C_i \equiv \{f_i = 0\}$ and let $\pi : X' \to X$ be a log-resolution of the product of all the f_i's, with $F_i := \pi^*C_i$. Fix a point $\boldsymbol{c} := (c_1, \dots, c_r) \in \mathbb{R}^r_{\geqslant 0}$ the corresponding *mixed multiplier ideal* is defined as

$$\mathcal{J}\left(C^{\boldsymbol{c}}\right) := \mathcal{J}\left(C_1^{c_1} \cdots C_r^{c_r}\right) = \pi_* \mathcal{O}_{X'}\left(\lceil K_\pi - c_1 F_1 - \cdots - c_r F_r \rceil\right) .$$

In the case $r = 1$, they are known as *multiplier ideals*.

It is important to note that as in the case of multiplier ideals, mixed multiplier ideals are complete for any tuple of curves and $\boldsymbol{\lambda}$.

Another definition that we need in this note is the following:

Definition 0.3. With the above notation, and given $\boldsymbol{\lambda} := (\lambda_1, \dots, \lambda_r) \in \mathbb{R}^r_{\geqslant 0}$, we define:

- The *region* of $\boldsymbol{\lambda}$ as: $\mathfrak{R}_{\boldsymbol{f}}(\boldsymbol{\lambda}) = \left\{ \boldsymbol{\lambda'} \in \mathbb{R}^r_{\geqslant 0} \,\middle|\, \mathcal{J}\left(\boldsymbol{f}^{\lambda'}\right) \supseteq \mathcal{J}\left(\boldsymbol{f}^{\lambda}\right) \right\}$

[1] Note that in the latter the k_i's are 0.

Contents

- The *constancy region* of $\boldsymbol{\lambda}$ as: $\mathfrak{C}_f(\boldsymbol{\lambda}) = \left\{\boldsymbol{\lambda'} \in \mathbb{R}^r_{\geqslant 0} \,\middle|\, \mathcal{J}\left(\boldsymbol{f}^{\lambda'}\right) = \mathcal{J}\left(\boldsymbol{f}^{\lambda}\right)\right\}$

The boundary of the region of $\boldsymbol{\lambda}$ is the *jumping wall*. In the case $r = 1$ this notion is the *jumping numbers*. It is important to note that as the multiplier ideals, they are independent of the chosen resolution. In order to describe the regions and jumping walls we need the following definitions:

Definition 0.4. Given a log-resolution $\pi : X' \longrightarrow X$ of X with exceptional divisors E_i, we define the following:

- Given two divisors D and D' in X', we will say that they are equivalent if they define the same complete ideal, i.e., $\pi_*\mathcal{O}_{X'}(-D) = \pi_*\mathcal{O}_{X'}(-D')$.
- A divisor D is *antinef* if $-D \cdot E_i \geqslant 0$, for all exceptional divisors E_i.
- Given a divisor D, there is a unique equivalent antinef divisor $\tilde{D}$ called *antinef closure* of D. This divisor $\tilde{D}$ is explicitly described by a procedure called unloading.
- We will say that E_i is a dicritical divisor for D if $-D \cdot E_i > 0$.

We are interested in dicritical divisors because of the following equivalence.

Theorem 0.5 (Lipman [8])**.** *There is a one-to-one correspondence between antinef divisors in $Div(X')$ and complete ideals in $\mathcal{O}_{X,O}$.*

As already mentioned, mixed multiplier ideals are complete ideals, so we can describe them by means of antinef divisors. We can therefore describe the regions as follows.

Theorem 0.6 (Alberich-Carramiñana, Àlvarez Montaner, Dachs-Cadefau [1])**.** *Let $\boldsymbol{f} := (\mathfrak{a}_1, \ldots, \mathfrak{a}_r)$ be a tuple of curves and let $D_{\boldsymbol{\lambda}} = \sum_{j=1}^s e_j^{\boldsymbol{\lambda}} E_j$ be the antinef closure of $\lfloor \lambda_1 F_1 + \ldots + \lambda_r F_r - K_\pi \rfloor$ for a given $\boldsymbol{\lambda} := (\lambda_1, \ldots, \lambda_r) \in \mathbb{R}^r_{\geqslant 0}$. Then the region of $\boldsymbol{\lambda}$ is the minimal convex polyhedron determined by*

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

with E_j either exceptional or non-exceptional, and $F_k = \sum_{i=1}^s e_{i,k} E_i$ and z_i are variables.

1. Topological type

In the case of analytically irreducible plane curves and by extension the case of simple ideals, there is a well-known relation between the equisingularity type and the jumping numbers.

Theorem 1.1 (Järvilehto, Thm 9.8 in [6])**.** *The jumping numbers of an analytically irreducible plane curve C which are less than one determine the equisingularity class of C.*

The proof of this Theorem is constructive, so given the jumping numbers, we can recover the equisingularity class of the curve. However this result does not hold when we drop the condition of being irreducible. For example, consider the following two curves (see [9]):

- $C_1 = \left\{(y^5 - x^2)(y^3 - x^2)(y^3 - x^4)(y^2 - x^7) = 0\right\}$, and
- $C_2 = \left\{(y^5 - x^2)(x^3 - y^2)(x^3 - y^4)(y^2 - x^7) = 0\right\}$.

Both of them have the same jumping numbers. A natural question would therefore be: do the jumping numbers of the germ of a plane curve determine the equisingularity classes of its branches (Tucker in [9])? Unfortunately the answer to this question is also negative. Consider the following example:

- $C_1 = \left\{(y^4 - 2x^3y^2 + x^6 - 4x^{10} - x^{17})(x^4 - 2x^2y^5 - 4xy^8 + y^{10} - y^{11}) = 0\right\}$, and
- $C_2 = \left\{(y^4 - 2x^3y^2 + x^6 - 4x^9y - x^{15})(x^4 - 2x^2y^5 + y^{10} - 4xy^9 - y^{13}) = 0\right\}$.

Both curves have the same jumping numbers, with the same multiplicities, and the branches composing C_1 are not equisingular to any branch composing C_2. It seems clear that we need another invariant than the jumping numbers in order to determine the equisingularity class. We could ask, what information could we get from the jumping walls? More precisely, given a set of jumping walls, under which assumptions can we determine the equisingularity class of all the curves associated to each axis and the product of all of them?

It seems clear that from Theorem 1.1 that each axis should represent an analytically irreducible curve, because if not, we cannot recover the equisingularity class of the branch. With this assumption, we can recover the equisingularity class of each of the branches, so the only missing piece of information is the intersection multiplicity. But this multiplicity can be recovered by the following result (see for example [3, Thm 4.5]).

Theorem 1.2. *The intersection multiplicity of two branches C_1 and C_2 is equal to the multiplicity of the branch C_1 in the exceptional divisor E_i such that $E_i \cdot \tilde{C}_2 \neq \emptyset$, where $\tilde{C}_2$ is the strict transform of C_2. Or equivalently, to the multiplicity of the branch C_2 in the exceptional divisor E_i such that $E_i \cdot \tilde{C}_1 \neq \emptyset$, where $\tilde{C}_1$ is the strict transform of C_1.*

Thanks to this result, we can state the following theorem that allows us to find the equisingularity class by means of the algorithm 1.4.

Theorem 1.3. *The jumping walls determine the equisingularity class of a tuple of curves.*

Algorithm 1.4. `Input:` The jumping walls of a tuple of curves.
`Output:` The equisingularity class of each of the curves and of the product of all of them.

- From the jumping numbers of each curve recover the equisingularity class by using the results of Järvilehto.
- From the last of the necessary jumping numbers for one of the branches, determine the equation of the facet of the jumping wall containing the jumping number. The intersection number with the other curves are the coefficients.

However, we can go a bit further, namely, as can be deduced from the algorithm and the proof of Theorem 1.3, we do not use all the information given by the jumping walls, in fact many of them are redundant. In fact, we need even less information:

Theorem 1.5. *The jumping numbers of a curve together with the jumping numbers of each pair of its branches determine its equisingularity class.*

So the equisingularity class can be found using the following algorithm.

Algorithm 1.6. `Input:` The jumping numbers of a curve together with the jumping numbers of each pair of its r branches.
`Output:` The equisingularity class of each of the branches and of the product of all of them.

- From the jumping numbers of each curve recover the equisingularity class by using the results of Järvilehto.
- Identify the first jumping number of the product that cannot be associated to a rupture, dicritical or non-exceptional divisor for one of the branches and with that determine the intersection multiplicity.[2]

[2]The details of this second step require some extra notions that can be found in [5].

Example 1.7. Assume that we have the jumping walls of Figure 1. From there, we can get the jumping numbers of both curves and of the product.

Once we have the jumping numbers, we find that the first curve has two Puiseux pairs, $\{2,3\},\{3,7\}$, and the second has $\{2,3\},\{4,11\}$.

If we want to use Algorithm 1.4, we have to pick the jumping number needed to determine the equisingularity class of one of the curves, namely $\frac{25}{66}$ for the first one. It is contained in the hyperplane $66z_1 + 84z_2 = 25$ and the intersection multiplicity is therefore 84. This means the product of C_1 and C_2 has the dual graph of Figure 2, where the rupture divisors are represented by white dots, while the strict transforms are represented by green dots.

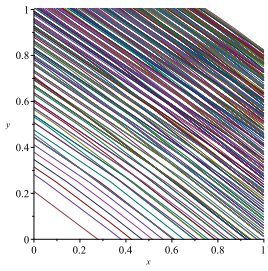


Figure 1: Jumping Walls

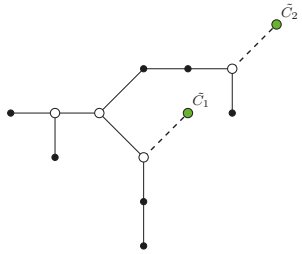


Figure 2: Dual graph of the product of C_1 and C_2.

If instead we use Algorithm 1.6, the jumping number of the product we are interested in is $\frac{8}{49}$, and this gives us, as expected, the same dual graph and the same intersection multiplicity, 84.

References

[1] M. Alberich-Carramiñana, J.Àlvarez Montaner and F. Dachs-Cadefau, *Constancy regions of mixed multiplier ideals in two-dimensional local rings with rational singularities.*, Mathematische Nachrichten, 291, (2018), 245-263.

[2] M. Alberich-Carramiñana, J.Àlvarez Montaner, F. Dachs-Cadefau and V. González-Alonso, *Multiplicities of jumping points of mixed multiplier ideals.*, Revista Matemática Complutense 33 (2020), no. 1, 325–348.

[3] E. Artal Bartolo, J. Martín-Morales, J. Ortigas-Galindo, *Intersection theory on abelian-quotient V-surfaces and Q-resolutions.*, J. Singul. 8 (2014), 11–30.

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

[5] F. Dachs-Cadefau, *Mixed multiplier ideals and equisingularity class*, in preparation, 2022.

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

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

[9] K. Tucker, *Jumping Numbers and Multiplier Ideals on algebraic surfaces* PhD Thesis (2010).

Martin-Luther-Universität Halle-Wittenberg
Institut für Mathematik
06099 Halle (Saale)
Email address: ferran.dachs-cadefau@mathematik.uni-halle.de

THE BENEFITS OF CLUSTERING IN CYLINDRICAL ALGEBRAIC DECOMPOSITION

TERESO DEL RÍO AND MATTHEW ENGLAND

Abstract. Cylindrical Algebraic Decomposition (CAD) is a very powerful algorithm with many potential applications. However, its doubly-exponential complexity limits its usability. In this document we demonstrate how the techniques of adjacency and clustering would reduce the double exponent of CAD complexity.

1. Introduction

Cylindrical Algebraic Decomposition (CAD), was introduced by Collins in [5]. Given an ordering in n variables (e.g. $x_1 \succ ... \succ x_n$) a CAD is a *decomposition* of $\mathbb{R}^n$ into cells (i.e. connected regions). These cells must be *semi-algebraic* and for any pair of cells their projections with respect to the given ordering are either equal or disjoint (*cylindricity*).

A CAD can be produced with respect to a set of polynomials in such a way that each of the polynomials is sign-invariant on each of the cells. This is very powerful, and in particular, it can be used to solve any Tarski formulae described by the given polynomials and any associated Real Quantifier Elimination problem, if an appropriate variable ordering is chosen.

CAD has been applied in a wide variety of problems, such as disproving an existent biological conjecture [9], analysing numerical schemes [11] and the "piano movers" problem [12]. However, CAD has a doubly-exponential worst case complexity in the number of variables [4], meaning that problems with many variables cannot yet be tackled. It is only thanks to 40 years of research that it is possible to apply CAD to the problems above [3].

One interesting improvement was introduced by Arnon in [1] in the early days of CAD. It consisted of clustering adjacent cells in which the sign of the given polynomials was invariant, to study them together. This idea brought savings in small examples, but at that time few algorithms to find adjacencies existed, and those that did were comparatively expensive. Over time, better projection algorithms were designed, reducing the amount of computations needed to build a CAD, and when using those new projections it was no longer possible to cluster using adjacency as presented in [1]. For these reasons, and perhaps because Arnon left academia, adjacency and clustering have not been major topics of CAD research and are not used in many CAD implementations.

However, the theory on finding adjacencies has improved since Arnon's original work, first with the local box algorithms of [7] and more recently the validated numerics approach of Strzebonski in [10], which gives a powerful and cheap algorithm to find adjacencies in CAD.

The first author is supported by Coventry University and the second by EPSRC grant EP/T015748/1: *Pushing Back the Doubly-Exponential Wall of Cylindrical Algebraic Decomposition* (DEWCAD)..

The presentation at EACA 2022 was given by the first author.

Strzebonski's results imply that the potential of clustering can be exploited if the necessary theory were extended to the modern projection algorithms such as [8]. In preparation and motivation for such developments, we present here the theoretical complexity benefits of clustering, namely a reduction in the double exponent of the worst case complexity bound.

2. Cylindrical Algebraic Decomposition

The CAD algorithm requires a variable ordering (e.g. $x_1 \succ ... \succ x_n$) and can be split into two phases: projection and lifting. In the projection phase, a projection operator is applied to a set of polynomials in n variables to obtain a set of polynomials without the largest variable in the ordering. This is done recurrently until a set of polynomials in one variable is found. The set of polynomials with only the first i variables will be denoted S_i.

This allows the next phase, the lifting phase. Here a CAD of $\mathbb{R}$ is built using S_1, then on top of it, a CAD of $\mathbb{R}^2$ is constructed using S_2, and we continue recursively until the desired CAD of $\mathbb{R}^n$ is obtained. The CAD of $\mathbb{R}^i$ will be denoted as CAD_i.

CAD_I is built from S_i and CAD_{i-1} by taking each cell of CAD_{i-1}, substituting its sample point into S_i, isolating roots, and inferring the behaviour in the whole cell from this analysis of the sample. In order for the cells generated in $\mathbb{R}^j$ to be sign-invariant we need to prove that the structure of the roots of S_i is invariant over the cell in CAD_{i-1}. This property is called delinability. The following theorem of Collins gives this assurance for his projection operator.

Theorem 2.1. *(Theorem 5 of [5]) Let $\mathcal{T}$ be a non-empty set of non-zero real polynomials in r real variables, $r \geq 2$. Let A be a connected subset of $\mathbb{R}^{r-1}$. Let $\mathcal{P}$ be the Collins projection of $\mathcal{T}$. If every element of $\mathcal{P}$ is sign-invariant on A, then the roots of $\mathcal{T}$ are delineable on A.*

More modern projection operators can achieve such a property with fewer polynomials. For example, the Lazard projector operator [8] satisfies the following theorem.

Theorem 2.2. *Let $\mathcal{T}$ be a non-empty set of non-zero real polynomials in r real variables, $r \geq 2$. Let A be a connected subset of $\mathbb{R}^{r-1}$. Let $\mathcal{P}$ be the Lazard projection of $\mathcal{T}$. If every element of $\mathcal{P}$ is Lazard valuation invariant on A, then the polynomials in $\mathcal{T}$ are Lazard analytic delineable on A.*

3. Adjacency and Clustering

In the theorems above, the projections satisfy neither cylindricity nor the semi-algebraic property over the region A: only connectedness is needed. In [1], Arnon took advantage of this by realizing that if two cells A and B are adjacent (i.e. their union is connected) and they share the same sign for all the relevant polynomials, then Theorem 2.1 could be applied to the union of those two cells $A \cup B$.

For example, in the CAD of $x^2 - y = 0$ depicted on in Figure 1, the blue two-dimensional cell and the purple one-dimensional cell have a connected union and share the same sign for the polynomial. This implies that in any further lifting phase we could cluster them and analyse them together rather than lifting over them separately. Moreover, the same reasoning applies for clustering the pink and the purple cell, and so on.

It is also possible to cluster together the two green one dimensional cells with the single point cell at the turning point of the curve. In total, we would be able to cluster the original 9 cells into 3 clusters, reducing by a third the effort needed to lift over this CAD.

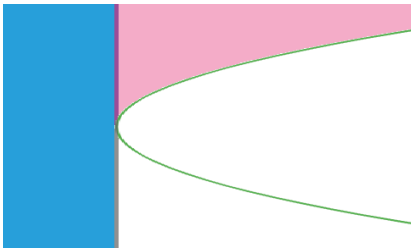


FIGURE 1. CAD of $x^2 - y = 0$ for the variable ordering $x \succ y$.

4. Complexity analysis

To give a complexity analysis of CAD we must understand how polynomial degrees grow during the projection phase. Given a set of polynomials that has a degree of most d in each of its variables, it is possible to show that the Lazard projection set of those polynomials has a degree of at most d^2 in each of its variables [6]. Likewise, it can be shown that the Collins projection set of those polynomials has a degree of at most d^6 in each.

This implies that if the original set of polynomials S_n has n variables and a degree of at most d on each of them, then the set S_i will have a degree of at most $d^{6^{n-i+1}}$ in each variable if Collins projection is used, and degree $d^{2^{n-i+1}}$ in each variable if Lazard projection is used.

The most expensive routine in the CAD algorithm is the real root isolation, and the number of root isolations needed to build a CAD is proportional to the number of cells generated. In order to study the worst case complexity of the CAD algorithm we can therefore+ study the maximum number of cells that can be generated.

It is important to note that if the number of cells of CAD_i is c_i and the sum of the total degrees of the biggest variable in S_{i+1} is d_{i+1} then the number of cells of CAD_{i+1} is $c_{i+1} \leq c_i(2d_{i+1} + 1)$ [6]. Applying this recursively, the maximum number of cells that can be generated including all the intermediate CADs is

$$\sum_{i=1}^{n} \prod_{j=1}^{i} (2d_j + 1),$$

resulting in an $\mathcal{O}(d^{\frac{6^n}{5}})$ worst case number of cells for Collins and $\mathcal{O}(d^{2^n})$ for Lazard.

However, using the upper bound of the number of sign-invariant connected components of a set of polynomials given in [2], it can be shown using Stirling's approximation that given a polynomial with a degree of at most d on each of its n variables the maximum number of sign-invariant clusters is of the order $\mathcal{O}(dn)^n$.

When clustering, the maximum number of cells that can therefore be generated including all the intermediate CADs is

$$2d_1 + 1 + \sum_{i=2}^{n} (2d_i + 1)(d_{i-1}i)^i,$$

resulting in $\mathcal{O}(d^{6^{n-1}})$ cells for Collins and $\mathcal{O}(d^{2^{n-1}})$ for Lazard.

5. Conclusion

The improvements, a reduction by one of the double exponent, might not look impressive at first glance, but are in fact significant in the context doubly-exponential growth. For example, in Lazard projection the maximum number of cells generated if clustering would be the square root of the maximum number of cells generated without using clustering. This means that for $n = 6$ we would build at most $4,294,967,296$ cells when clustering compared to the $18,446,744,073,709,551,616$ without using clustering.

Furthermore, when clustering is not employed the number of cells in an intermediate CAD is a multiple of the number of cells in the previous CAD. However, when using clustering that is not necessarily the case, and the number of cells could decrease in some cases.

Finally, it is important to note that considering that the computations of adjacencies did not have a significant effect with respect to the cost of the CAD in [10], the usage of clustering to create a CAD would be very unlikely to slow down the process.

We hope this helps motivate the CAD community to bring Arnon's idea back to the forefront of CAD research, so that it can be coupled with the other achievements, and further push back the doubly-exponential wall of CAD!

References

1. Dennis S. Arnon, George E. Collins, and Scott McCallum, *Cylindrical Algebraic Decomposition II: An Adjacency Algorithm for the Plane*, SIAM Journal on Computing **13** (1984), no. 4, 878–889.
2. Sal Barone and Saugata Basu, *Refined Bounds on the Number of Connected Components of Sign Conditions on a Variety*, Discrete Comput Geom (2012), no. 47, 577–597.
3. Russell Bradford, James H. Davenport, Matthew England, Amir Sadeghimanesh, and Ali Uncu, *The DEWCAD Project: Pushing Back the Doubly Exponential Wall of Cylindrical Algebraic Decomposition*, ACM Communications in Computer Algebra **55** (2021), no. 3, 107–111.
4. Christopher W. Brown and James H. Davenport, *The complexity of quantifier elimination and cylindrical algebraic decomposition*, ISSAC (2007), 54–60.
5. George E. Collins, *Quantifier elimination for real closed fields by cylindrical algebraic decomposition*, Lecture Notes in Computer Science **33** (1975), 134–183.
6. Matthew England and James H. Davenport, *The complexity of cylindrical algebraic decomposition with respect to polynomial degree*, Computer Algebra in Scientific Computing (2016), 172–192.
7. Scott McCallum and George E. Collins, *Local box adjacency algorithms for cylindrical algebraic decompositions*, Journal of Symbolic Computation **33** (2002), no. 3, 321–342.
8. Scott McCallum, Adam Parusiński, and Laurentiu Paunescu, *Validity proof of Lazard's method for CAD construction*, Journal of Symbolic Computation **92** (2019), 52–69.
9. Gergely Röst and Amirhosein Sadeghimanesh, *Exotic Bifurcations in Three Connected Populations with Allee Effect*, International Journal of Bifurcation and Chaos **31** (2021), no. 13, 2150202.
10. Adam Strzeboński, *CAD adjacency computation using validated numerics*, ISSAC (2017), 413–420.
11. Stefan Takacs, *Using cylindrical algebraic decomposition and local Fourier analysis to study numerical methods: two examples*, SYNASC (2014), 42–49.
12. David Wilson, James H. Davenport, Matthew England, and Russell Bradford, *A "piano movers" problem reformulated*, SYNASC (2013), 53–60.

Coventry University, Coventry, UK.
Email address: delriot@coventry.ac.uk, Matthew.England@coventry.ac.uk

FASTER KENZO COMPUTATIONS VIA SAGEMATH, AND VICE VERSA

JOSE DIVASÓN, MIGUEL MARCO BUZUNÁRIZ, AND ANA ROMERO

Abstract. This work presents some improvements on the efficiency of both Kenzo and SageMath, by means of parallelization techniques and an existing interface that connects both systems.

Introduction

Kenzo [2] is a computer algebra system devoted to algebraic topology which in particular implements several algorithms to compute homology groups of infinite structures using the method of effective homology [4]. In addition, it also permits homotopy groups to be computed algorithmically combining the Whitehead tower method [5] and the effective homology technique. As far as we know, Kenzo is the only program able to carry out this kind of computations on infinite structures, which makes it a powerful software. In order to increase and ease the use of Kenzo, we developed an interface and an optional package of Kenzo within Sagemath [1]. That work permitted the use of Kenzo and some of its external packages without any Common Lisp knowledge, and enhanced the SageMath system with new capabilities in algebraic topology (dealing in particular with simplicial objects of infinite nature).

In this work, we improve the efficiency of our Kenzo–SageMath interface by combining the power of both computer algebra systems, considering in particular the computation of homology groups. On the one hand, we use parallel computations in SageMath (using multiprocessing in Python) to accelerate Kenzo computations. On the other hand, Kenzo can improve SageMath capabilities beyond topological computations. One such example is the Smith normal form of an integer matrix, for which Kenzo provides a faster implementation than Pari (which is what SageMath uses).

1. Computation of homology groups in Kenzo

The computation of homology groups in Kenzo is performed by means of the effective homology method [4]. When an object (e.g., a simplicial set) X is built in Kenzo, a particular case of homology equivalence $C_*(X) \Longleftrightarrow E_*$ is automatically constructed, where $C_*(X)$ is the chain complex associated with X and E_* is a chain complex of finite type (called effective) such that its homology groups are isomorphic to those of C_*, $H_*(C) \cong H_*(E)$. Since E_* is finitely generated in each degree, the homology groups of E_* can be determined

The first and third author are supported by grant PID2020-116641GB-I00 funded by MCIN/ AEI/ 10.13039/501100011033. The second author has been partially supported by PID2020-114750GB-C31 and E22_20R: Álgebra y Geometría.

The talk at the EACA 2022 meeting was given by the third author.

by means of elementary operations on matrices. In this way, the homology groups of the object X, which can be of infinite nature, can also be determined (thanks to the isomorphism $H_*(X) \cong H_*(C_*(X)) \cong H_*(E)$). Given a chain complex C_*, its homology groups $H_n(C_*)$ are defined as $H_n(C_*) = \operatorname{Ker} d_n / \operatorname{Im} d_{n+1}$, where d_* denotes the differential map of the complex. These groups are determined in Kenzo by means of the following algorithm.

Algorithm 1: Homology groups of a chain complex.

Input: A chain complex C_* with effective homology and an integer n.
Output: The homology group $H_n(C_*)$.

1 Consider the effective chain complex associated with C_*, denoted E_*.
2 Construct the differential matrix of E_* of degree n, denoted D_n.
3 Construct the differential matrix of E_* of degree $n+1$, denoted D_{n+1}.
4 Compute the kernel of D_n, denoted K_n, by diagonalization techniques [3].
5 Return the quotient of K_n by D_{n+1}, by again using diagonalization techniques.

Using profiling, we detected that 99% of the required time was devoted to instructions in lines 2 and 3 of Algorithm 1, i.e., determining the differential matrices of the effective chain complex. This is due to the fact that these matrices are built by determining the image of the differential map of each generator of the chain complex E_* on the required degrees, and the differential morphisms of the effective chain complex E_* are constructed by means of complicated maps describing the effective homology of the object [4].

2. Improving Kenzo and SageMath

The existing interface between SageMath and Kenzo [1] connects both programs via the ECL library (a library interface to Embeddable Common Lisp), which is itself loaded as a C-library. This enables the interface to be very fast, and the efficiency between native Kenzo and Kenzo loaded in Sagemath is similar. The idea of this work is to exploit both systems to improve the efficiency of computations. All the code is publicly available at `https://github.com/jodivaso/EACA22`.

2.1. **Improving Kenzo via SageMath.**

We applied parallelization techniques to Kenzo thanks to the SageMath interface, i.e., we use existing multiprocessing Python libraries to run parallel computations in Kenzo. Unlike other programming languages, Python multithreading (via `threading` and `asyncio` Python packages) does not allow parallelization, but only concurrency. This is due to the existence of a Global Interpreter Lock (GIL), whose purpose is to allow only one thread to hold the control of the Python interpreter. The standard way to run a task in Python in parallel is therefore by means of independent subprocesses, without sharing memory among them. However, programmers need to somehow share objects between subprocesses (for example, to share the input matrix with the subprocess that will compute something of it). This is solved thanks to serialization (or *pickle* in Python jargon): the process whereby a Python object is converted into bytes. If the main process needs to send two different matrices to two subprocesses (like if we parallelize lines 2 and 3 in Algorithm 1), then two serializations are performed (one for each matrix). The matrices are then unpickled in the subprocesses, computation is performed in each subprocess, and the results are also serialized and finally unpickled in the main process.

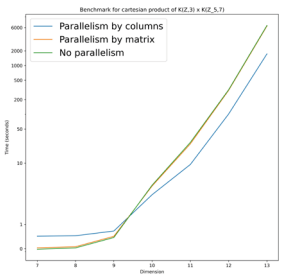
The Kenzo interface defines the class `KenzoObject`, which is simply a wrapper in Sage around a Kenzo object, i.e., it only contains an `EclObject`. However, pickling over an `EclObject` is not supported, since ECL does not natively support serialization of its objects. To overcome this limitation, we have now added an attribute named `command`, in which we store how the object has been built. This variable stores the commands to reconstruct the Kenzo object by means of Python code (which internally will run Lisp code thanks to the interface). `KenzoObject` now has two attributes: the `EclObject` already built and the `command` to build it. We do this for each object that can be constructed in Kenzo via the interface (Cartesian product, wedge, loop space, join, spheres, ...).

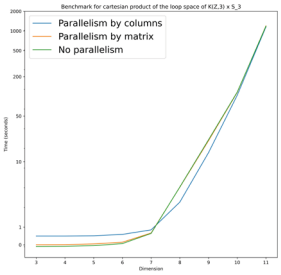
To serialize a `KenzoObject` (as well as any of its inherited classes, like `KenzoChainComplex`) the trick is to define our own method to serialize (pickle), which will only serialize the `command`, but not the `EclObject`. We also defined the deserializing method (unpickle), where the command is executed to reconstruct the `EclObject`. We can therefore input and output `KenzoObjects` between processes. We parallelize Algorithm 1 in two ways:

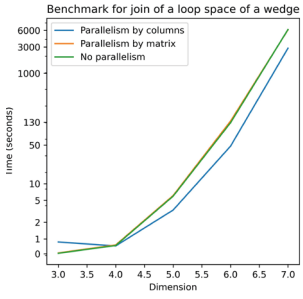
(1) Computing D_n and D_{n+1} in two different processes (parallelism by matrices).
(2) Separately computing the columns of D_n and D_{n+1} in m processes, and then reconstructing D_n and D_{n+1} (parallelism by columns).

The former is done by means of `multiprocessing.pool`. Only Python code is necessary to obtain parallelism. The latter requires to develop new Lisp code that, given E_*, a degree k and two indexes i and j, computes the columns from i to j of D_k. Additionally, we also have an optional parameter to select the number of cores to use (to maximize the performance, by default is set to the available number of logical cores). Finally, we reconstruct each of the matrices from their columns and continue with the process.

Our benchmarks show that execution times improve noticeably, although it depends on the space. For instance, to compute the homology in dimension 13 of the cartesian product of the Eilenberg–MacLane spaces $K(\mathbb{Z}, 3)$ and $K(\mathbb{Z}/5\mathbb{Z}, 7)$ requires 6627.8s without doing any parallelism, 6457.28s using the parallelism by matrices and 1734.5s using parallelism by columns. The computing time is thus reduced by around 75% in such an example.







The figures presented above show the execution times (on a logarithmic scale) of the computation of homology in different dimensions of:

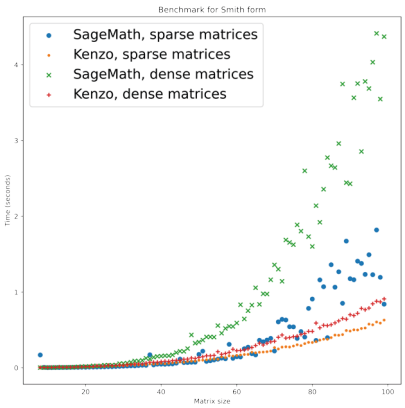
(1) Cartesian product of the Eilenberg–MacLane spaces $K(\mathbb{Z}, 3)$ and $K(\mathbb{Z}/5\mathbb{Z}, 7)$.
(2) Cartesian product of the loop space of the Eilenberg–MacLane space $K(\mathbb{Z}, 3)$ and the 3-sphere.

(3) Join product of S and the loop space of S, where S is the wedge of a 2-sphere and a 3-sphere.

The figures show that computing times do not improve greatly using parallelism by matrices. This is due to the fact that the computation of D_{n+1} is usually much harder than D_n, consuming most of the time. Parallelization by columns improves computation times with respect to the version with no parallelism, and in most cases in a notably manner. The exception is in low dimensions, whose execution is almost immediate (less than one second). In those cases it is slower due to the overhead of running subprocesses, serializations and so on. The experiments have been performed on an Intel i7-4790, with 8 logical cores. In principle, we could expect to reduce the computing time by a factor of 8, but in this problem it is not possible since the computation of each column does not require the same time: some of them are harder and cause the bottleneck. Nevertheless, the improvement is important.

2.2. **Improving SageMath via Kenzo.** Kenzo relies on the Smith form of integer matrices for its computations. As a result, it includes an optimized implementation. With the appropriate glue code, Kenzo implementation can be used from SageMath. We compared the performance of this approach with the native SageMath implementation (provided by Pari).

It can be seen that Kenzo implementation is clearly faster than native SageMath, for both dense and sparse matrices. The difference for matrices of size 100 is about one order of magnitude. Kenzo has also much more predictable timings.



References

1. Julián Cuevas-Rozo, Jose Divasón, Miguel Marco-Buzunáriz, and Ana Romero, *Integration of the Kenzo system within SageMath for new algebraic topology computations*, Mathematics **9** (2021), no. 7.
2. X. Dousson, J. Rubio, F. Sergeraert, and Y. Siret, *The Kenzo program*, `http://www-fourier.ujf-grenoble.fr/~sergerar/Kenzo/`, 1999.
3. T. Kaczynski, K. Mischaikow, and M. Mrozek, *Computational homology*, Applied Mathematical Sciences, vol. 157, Springer, 2004.
4. J. Rubio and F. Sergeraert, *Constructive Homological Algebra and Applications, Lecture Notes Summer School on Mathematics, Algorithms, and Proofs*, University of Genova, 2006, `http://www-fourier.ujf-grenoble.fr/~sergerar/Papers/Genova-MAP-2006-v3.pdf`.
5. G. Whitehead, *Fiber spaces and the Eilenberg homology groups*, Proceedings of the National Academy of Science of the United States of America **38** (1952), no. 5, 426–430.

University of La Rioja. c/Madre de Dios 53. 26006 Logroño, Spain.
Email address: `jose.divason@unirioja.es`

Universidad de Zaragoza/IUMA.
Email address: `mmarco@unizar.es`

University of La Rioja. c/Madre de Dios 53. 26006 Logroño, Spain.
Email address: `ana.romero@unirioja.es`

THE LEVEL OF A POLYNOMIAL, AND SOME REASONS TO CARE ABOUT IT

ALBERTO F. BOIX

Abstract. The goal of this survey is to review several recent results concerning the level of a polynomial, and to see how it is related with notions coming from Number and Singularity Theory.

Introduction

Let k be any perfect field and $R = k[x_1, ..., x_d]$ its polynomial ring in d variables. In this case it is known [Gro67, IV, Théorème 16.11.2] that the ring $\mathcal{D}_R$ of k–linear differential operators on R is the R-algebra (which we take here as a definition)

$$\mathcal{D}_R := R\langle D_{x_i,t} \mid i = 1, \dots, d \text{ and } t \geq 1\rangle \subseteq \mathrm{End}_k(R),$$

generated by the operators $D_{x_i,t}$, defined as

$$D_{x_i,t}(x_j^s) = \begin{cases} \binom{s}{t} x_i^{s-t}, \text{ if } i = j \text{ and } s \geq t, \\ 0, \text{ otherwise .} \end{cases}$$

For a non-zero $f \in R$, let R_f be the localization of R at f; the natural action of $\mathcal{D}_R$ on R extends in a unique way to R_f and it is known that $m \geq 1$ exists such that $R_f = \mathcal{D}_R \frac{1}{f^m}$. In characteristic 0 there are examples where the minimal such that m is strictly larger than 1 (e.g. [ILL$^+$07, Example 23.13]). On the other hand, if $\mathrm{char}(k) = p > 0$ one may always take $m = 1$ ([ÀMBL05, Theorem 3.7 and Corollary 3.8]). This is shown by proving the existence of a differential operator $\delta \in \mathcal{D}_R$ such that $\delta(1/f) = 1/f^p$, i.e., δ acts as Frobenius on $1/f$.

We will suppose that k is a perfect field with a positive characteristic p. For an integer $e \geq 0$, let $R^{p^e} \subseteq R$ be the subring of all the p^e powers of all the elements of R and set $\mathcal{D}_R^{(e)} := \mathrm{End}_{R^{p^e}}(R)$, the ring of R^{p^e}-linear ring-endomorphism of R. Since R is a finitely generated R^p-module, by [Yek92, 1.4.8 and 1.4.9], it is

$$\mathcal{D}_R = \bigcup_{e \geq 0} \mathcal{D}_R^{(e)}.$$

Therefore, for $\delta \in \mathcal{D}_R$, there exists $e \geq 0$ such that $\delta \in \mathcal{D}_R^{(e)}$ but $\delta \notin \mathcal{D}_R^{(e')}$ for any $e' < e$. This number e is called the level of δ. For a polynomial f, the level is defined as the lowest level of an operator δ such that $\delta(1/f) = 1/f^p$.

Date: February 20, 2023.

2010 *Mathematics Subject Classification.* Primary 13A35; Secondary 13N10, 14B05.

Key words and phrases. Algorithm, Differential operator, Frobenius map, Prime characteristic.

Alberto F. Boix is partially supported by Spanish Ministerio de Economía y Competitividad grant PID2019-104844GB-I00.

Contents

The goal of this survey is to review several recent results concerning the level of a polynomial, and to see how they are related with notions coming from Number and Singularity Theory.

1. How to calculate the level?

In order to provide effective tools for computing the level of a polynomial, we now review the so–called ideal of p^e–th roots.

Definition 1.1. Given $g \in R$ and an integer $e \geq 0$, we define the *ideal of p^eth roots* $I_e(g)$ as the smallest ideal $J \subseteq R$ such that $g \in J^{[p^e]}$.

Remark 1.2. Under our assumptions, R is a free R^{p^e}-module with basis given by the monomials $\{\mathbf{x}^\alpha \mid ||\alpha|| \leq p^e - 1\}$. A polynomial $g \in R$ can therefore be written as

$$g = \sum_{0 \leq ||\alpha|| \leq p^e - 1} g_\alpha^{p^e} \mathbf{x}^\alpha,$$

for unique $g_\alpha \in R$. Then $I_e(g)$ is the ideal of R generated by elements g_α [BMS08, Proposition 2.5].

The next result says that we can use ideals of p^e–th roots to calculate the level; more precisely:

Proposition 1.3. *The descending chain $R = I_0(f^{p^0-1}) \supseteq I_1(f^{p-1}) \supseteq I_2^{f^{p^2-1}} \supseteq \dots$ stabilizes rigidly, i.e., there is a minimal $e \geq 1$ such that $I_{e-1}(f^{p^{e-1}-1}) = I_{e+t}(f^{p^{e+t-1}-1})$ for any integer $t \geq 0$. Moreover,* $\operatorname{level}(f) = e = \min\{s \geq 1 : \ f^{p^s-p} \in I_s(f^{p^s-1})^{[p^s]}\}$.

2. An algorithm to compute the level

Let k be a computable perfect field of prime characteristic p (e.g., k is finite). Let $R = k[x_1, \dots, x_d]$, and let $f \in R$ be a non-zero polynomial. We now describe an algorithm that computes not only the level of f, but also a differential operator $\delta \in \mathcal{D}_R$ such that $\delta(1/f) = 1/f^p$. The interested reader may wish to consult [BDSV15] for further details.

- **Step 1.** Find the smallest integer $e \in \mathbb{N}$ with the property that $I_e(f^{p^e-p}) = I_{e-1}(f^{p^{e-1}-1}) = I_e(f^{p^e-1})$.
- **Step 2.** For $e \in \mathbb{N}$ as in **Step 1** write $f^{p^e-1} = \sum_{i=1}^n c_i^{p^e} \mu_i$, where $\{\mu_1, \dots, \mu_n\}$ is the basis of R as an R^{p^e}-module consisting of all the monomials $x_1^{a_1} \cdots x_d^{a_d}$, with $a_i \leq p^e - 1$ for all $i = 1, \dots, d$. In this situation, we can see that, for all $i = 1, \dots, n$, there is $\delta_i \in \mathcal{D}_R^{(e)}$ such that $\delta_i(\mu_j) = 1$ if $i = j$ and $\delta_i(\mu_j) = 0$ if $i \neq j$.
- **Step 3.** Since $1 \in \mathcal{D}_R^{(e)}$, for $e \in \mathbb{N}$ as in **Step 1** we have

  $$f^{p^e-p} \in \mathcal{D}_R^{(e)}(f^{p^e-p}) = I_e(f^{p^e-p})^{[p^e]} = I_e(f^{p^e-1})^{[p^e]} = (c_1, \dots, c_n)^{[p^e]}.$$

  In particular there is $\alpha_1, \dots, \alpha_n \in R$ such that $f^{p^e-p} = \sum_{i=1}^n \alpha_i c_i^{p^e}$. Let $\delta_i \in \mathcal{D}_R^{(e)}$ as in **Step 2**, so that $\delta_i(f^{p^e-1}) = c_i^{p^e}$, and set $\delta := \sum_{i=1}^n \alpha_i \delta_i \in \mathcal{D}_R^{(e)}$. With this choice

we have

$$\delta(f^{p^e-1}) = \delta\left(\sum_{j=1}^{n} c_j^{p^e}\mu_j\right) = \sum_{i,j=1}^{n} c_j^{p^e}\alpha_i\delta_i(\mu_j) = \sum_{i=1}^{n}\alpha_i c_i^{p^e} = f^{p^e-p},$$

and using $\delta \in \mathcal{D}_R^{(e)}$ we finally obtain $\delta(1/f) = (1/f)^p$.

3. The level of an elliptic curve

In this section, let $f \in \mathbb{F}_p[x,y,z]$ be a cubic homogeneous polynomial such that $E := V(f)$ is an elliptic curve over $\mathbb{F}_p$; it is known that we can write $f^{p-1} = c(xyz)^{p-1} + \dots$ for some $c \in \mathbb{F}_p$. In this way, we can say that E is *ordinary* if $c \neq 0$, and *supersingular* otherwise. It turns out that $\text{level}(f)$ gives a full characterization on whether E is ordinary or supersingular.

Theorem 3.1. *(*[BDSV15, Theorem 1.1]*) E is ordinary if and only if* $\text{level}(f) = 1$; *on the other hand, E is supersingular if and only if* $\text{level}(f) = 2$.

4. The level of an hyperelliptic curve

Theorem 3.1 was generalized for hyperelliptic curves of arbitrary genus $g \geq 2$; indeed, let $\mathcal{C} := \{(x : y : z) \in \mathbb{P}^2_{\mathbb{F}_p} : f(x,y,z) = 0\}$, where f is a homogeneous polynomial of degree $2g+1$ defined over $\mathbb{F}_p$. If $\text{Jac}(\mathcal{C})$ denotes its Jacobian, then it is well known [Mum08, Proposition on page 60] that for any integer $n > 0$,

$$\text{Jac}(\mathcal{C})[n](\overline{\mathbb{F}_p}) = \begin{cases} (\mathbb{Z}/n\mathbb{Z})^{2g} \text{ if } \text{char}(k) \nmid n, \\ (\mathbb{Z}/p^m\mathbb{Z})^i \text{ if } n = p^m,\ p = \text{char}(k) \text{ and } m > 0, \end{cases}$$

where i can take every value in the range $0 \leq i \leq g$, and is called the p-rank of $\mathcal{C}$.

Definition 4.1. The curve $\mathcal{C}$ is said to be ordinary if its p-rank is maximal, i.e., equal to the genus of $\mathcal{C}$. The curve $\mathcal{C}$ is said to be supersingular (resp. superspecial) if $\text{Jac}(\mathcal{C})$ is isogenous (resp. isomorphic) over $\overline{\mathbb{F}_p}$ to the product of g supersingular elliptic curves.

The generalization of Theorem 3.1 reads as follows [BCBFY18, Theorems 1.3, 3.5 and 3.9]:

Theorem 4.2. *Let $f \in R$ be a homogeneous polynomial in three variables and of degree $2g+1$, such that $\mathcal{C} \cong V(f) \subset \mathbb{P}^2$ defines a hyperelliptic curve over $\overline{\mathbb{F}_p}$ of genus g, and assume $p > 2g^2 - 1$. Then:*

(i) $\text{level}(f) = 2$ *if $\mathcal{C}$ is ordinary,*
(ii) $\text{level}(f) > 2$ *if $\mathcal{C}$ is supersingular but not superspecial.*

5. The level of a pair of polynomials

In [BNT20], the authors propose the following generalization of the level of a polynomial.

Definition 5.1. Given polynomials f, g with coefficients in a field k of prime characteristic p and $f \neq 0$, we define the *level of* (g,f) as

$$\text{level}(g,f) := \inf\{e \geq 0 :\ \exists \delta \in \mathcal{D}^{(e)} \text{ such that } \delta(g/f) = (g/f)^p\} \in \mathbb{N}_0 \cup \{\infty\}.$$

When $g = 1$, we denote level(f) instead of level$(1, f)$; this is the notion of level of a polynomial introduced in [BDSV15, Definition 2.6].

In contrast to what happens when $g = 1$, in general the level of a pair is not always finite.

Example 5.2. ([BNT20, Proposition 4.9]) Let $R = \mathbb{F}_p[x, y]$, and let $f = x^{p+1} + y^{p+1}$ and $g = x$. Then level$(g, f) = \infty$. In particular, no $\delta \in \mathcal{D}_R$ exists with $\delta(g/f) = g^p/f^p$.

6. Some final remarks

In Section 2 we introduce an algorithm to calculate the level; in [BHK+19] the authors present an alternative method for computing it in terms of local cohomology. It is also possible [For18] to compute the level of a polynomial f in terms of the F–jumping numbers of the hypersurface defined by f.

References

[ÀMBL05] J. Àlvarez Montaner, M. Blickle, and G. Lyubeznik. Generators of D-modules in positive characteristic. *Math. Res. Lett.*, 12(4):459–473, 2005.

[BCBFY18] I. Blanco-Chacón, A. F. Boix, S. Fordham, and E. S. Yilmaz. Differential operators and hyperelliptic curves over finite fields. *Finite Fields Appl.*, 51:351–370, 2018.

[BDSV15] A. F. Boix, A. De Stefani, and D. Vanzo. An algorithm for constructing certain differential operators in positive characteristic. *Matematiche (Catania)*, 70(1):239–271, 2015.

[BHK+19] A. F. Boix, D. J. Hernández, Z. Kadyrsizova, M. Katzman, S. Malec, M. Robinson, K. Schwede, D. Smolkin, P. Teixeira, and E. E. Witt. The TestIdeals package for Macaulay2. *J. Softw. Algebra Geom.*, 9(2):89–110, 2019.

[BMS08] M. Blickle, M. Mustaţă, and K. E. Smith. Discreteness and rationality of F-thresholds. *Michigan Math. J.*, 57:43–61, 2008.

[BNT20] A. F. Boix, M. P. Noordman, and J. Top. The level of pairs of polynomials. *Comm. Algebra*, 48(10):4235–4248, 2020.

[For18] S. Fordham. On the level of a Calabi–Yau hypersurface. Available at https://arxiv.org/pdf/1801.04893.pdf, 2018.

[Gro67] A. Grothendieck. Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas IV. *Inst. Hautes Études Sci. Publ. Math.*, (32):361, 1967.

[ILL+07] S. B. Iyengar, G. J. Leuschke, A. Leykin, C. Miller, E. Miller, A. K. Singh, and U. Walther. *Twenty-four hours of local cohomology*, volume 87 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2007.

[Mum08] D. Mumford. *Abelian varieties*, volume 5 of *Tata Institute of Fundamental Research Studies in Mathematics*. Published for the Tata Institute of Fundamental Research, Bombay; by Hindustan Book Agency, New Delhi, 2008. With appendices by C. P. Ramanujam and Yuri Manin, Corrected reprint of the second (1974) edition.

[Yek92] A. Yekutieli. An explicit construction of the Grothendieck residue complex. *Astérisque*, (208):127, 1992. With an appendix by Pramathanath Sastry.

IMUVA–Mathematics Research Institute, Universidad de Valladolid, Paseo de Belen, s/n, 47011, Valladolid, Spain.

Email address: alberto.fernandez.boix@uva.es

ON THE RANK OF POWERS OF A NON-DEGENERATE QUADRATIC FORM

COSIMO FLAVI

ABSTRACT. A decomposition of a homogeneous polynomial is a representation of that polynomial as a sum of powers of linear forms; in particular, the minimum number of addends in this sum is said to be the rank of the polynomial. We analyze a way to determine explicit decompositions of a polynomial corresponding to a power of a non-degenerate quadratic form. The main instrument used in this context is the Apolarity Lemma, which is a classic result relating the summands of a decomposition to its apolar ideal.

INTRODUCTION

Tensor decomposition has many applications in several scientific areas, such as psychology, geophysics and medicine (see [4, Chapter 1] for further details). This subject has recently begun to be addressed by using methods of algebraic geometry.

Considering a finite-dimensional vector space V with $\dim V = n$, defined in a field $\mathbb{K}$ such that $\mathrm{char}(\mathbb{K}) = 0$, its *d-th tensor power* can be described as the space

$$V^{\otimes d} = \mathrm{span}\{\, v_1 \otimes \cdots \otimes v_d \mid v_1, \ldots, v_d \in V \,\}.$$

Given a tensor $f \in V^{\otimes d}$, the natural number given by

$$\mathrm{rk}(f) = \min\left\{ r \in \mathbb{N} \;\middle|\; g = \sum_{j=1}^{r} v_{j,1} \otimes \cdots \otimes v_{j,d} : v_{j,i} \in V \right\}$$

is said to be the *rank* of the tensor f.

An important subspace of $V^{\otimes d}$ is represented by the *d-th symmetric power of* V, which can be identified as the vector space

$$S^d V = \mathrm{span}\left\{ v^{\otimes d} \;\middle|\; v \in V \right\}$$

and, analogously, we define the *symmetric rank* of a symmetric tensor $g \in S^d V$ as the natural number given by

$$\mathrm{rk}_S(h) = \min\left\{ r \in \mathbb{N} \;\middle|\; h = \sum_{j=1}^{r} v_j^{\otimes d} : v_j \in V \right\}.$$

Now, fixing an arbitrary basis of V, it is quite simple to show that the *symmetric algebra* of the space V, which is the direct sum

$$S(V) = \bigoplus_{d \in \mathbb{N}} S^d V,$$

is isomorphic to the ring of polynomials $\mathcal{R} = \mathbb{K}[x_1, \ldots, x_n]$. This means that it is possible to define in a natural way the *rank* of a polynomial, corresponding to the natural number

$$\mathrm{rk}(h) = \min\left\{ r \in \mathbb{N} \;\middle|\; h = \sum_{j=1}^{r} (a_{1,j}x_1 + \cdots + a_{n,j}x_n)^d : a_{i,j} \in \mathbb{K} \right\}.$$

Contents

The problem of the determination of the rank of a polynomial, also known as the *Waring rank*, has been a central issue in classical algebraic geometry and it is particularly important for the main applications of the theory of symmetric tensors.

1. Objectives

The main object analyzed in this context corresponds to the non-degenerate quadratic form

$$q_n = x_1^2 + \cdots + x_n^2,$$

defined on the field $\mathbb{C}$. The goal is therefore to determine some suitable decompositions of its powers. In other words, we aim to write some explicit decompositions as a sum of $2s$-powers of linear forms of the homogeneous polynomial

$$q_n^s = \left(x_1^2 + \cdots + x_n^2\right)^s,$$

trying to point out the minimal ones, establishing its rank.

This represents a classic problem, already addressed by B. Reznick in [5], in which he provides some of its real decompositions for specific values assumed by n and s.

In the case of two variables, such that $n = 2$, it is quite simple. In that case we easily obtain

$$\operatorname{rk} q_n^s = s + 1$$

and the coefficients of the linear forms constituting the decompositions obtained by B. Reznick correspond exactly to the coordinates of the vertices of regular $2s$-gon, clearly considered as projective points.

In the case of three variables, that is $n = 3$, B. Reznick shows some minimal real decompositions for the values $s = 1, 2, 3, 4$. By analyzing the disposition of the set of points in these first decompositions, we can observe some kind of symmetry in how they are arranged. In particular, for $s = 1$ the points represent the vertices of a regular octahedron, for $s = 2$ we obtain the vertices of a regular icosahedron and finally, for $s = 4$, the points of the decomposition form correspond to an icosahedron and a dodecahedron together. With this, the main idea is to try to generalize these arrangements of points, possibly observing common features.

2. Methodology

The tools purposed to be used are related to apolarity theory, the details of which can be found in [3]. Considering the symmetric algebras respectively of V and its dual space V^*, denoted by

$$\mathcal{R} = \mathbb{K}[x_1, \ldots, x_n] \simeq S(V), \quad \mathcal{D} = \mathbb{K}[y_1, \ldots, y_n] \simeq S(V^*),$$

the *apolarity action* of $\mathcal{D}$ on $\mathcal{R}$ is defined on the monomials by

$$\begin{aligned} \circ \colon \mathcal{D} \times \mathcal{R} &\longrightarrow \mathcal{R} \\ \left(\mathbf{y}^\alpha, \mathbf{x}^\beta\right) &\mapsto \frac{\partial}{\partial \mathbf{x}^\alpha}\left(\mathbf{x}^\beta\right). \end{aligned}$$

Moreover, for every homogeneous polynomial $h \in \mathcal{R}_d$, the *catalecticant map* of h is the map

$$\begin{aligned} \operatorname{Cat}_h \colon \mathcal{D} \times \mathcal{R} &\longrightarrow \mathcal{R} \\ g &\longmapsto g \circ h. \end{aligned}$$

Now, the kernel of this map, which is called the *apolar ideal* of the polynomial h and is denoted by

$$h^{\perp} = \mathrm{Ker}(\mathrm{Cat}_h),$$

is the main instrument we aim to use to determine some suitable decomposition of the form q_n^s, by using a very important related result, that is the Apolarity Lemma.

Lemma 2.1 (Apolarity Lemma)**.** *Let $A = \{[L_1], \dots, [L_r]\} \subset \mathbb{P}\big(S^1V\big)$ and $h \in S^dV$. Then the following conditions are equivalent:*
(i) $h = \sum_{i=1}^{r} a_i L_i^d$, *for some* $a_1, \dots, a_r \in \mathbb{K}$;
(ii) $\mathcal{I}(A) \subseteq h^{\perp}$.

This permits us to identify the decompositions of q_n^s as sets of points whose ideal is contained in $(q_n^s)^{\perp}$.

Using the representations presented by B. Reznick, once we have analyzed in detail how the apolar ideal of q_n^s is structured, it would be possible to consider its decompositions as the zero-dimensional variety and focus on a suitable characteristic of the subspace generating the corresponding ideals.

3. Results

Considering the Laplace operator

$$\Delta = \sum_{j=1}^{n} \frac{\partial^2}{\partial y_j^2}$$

and for each $d \in \mathbb{N}$, the space of harmonic homogeneous polynomials of degree d on $\mathbb{C}$, given by

$$\mathcal{H}_n^d(\mathbb{C}) = \{\, h \in \mathbb{C}[y_1, \dots, y_n] \mid \Delta h = 0 \,\},$$

it is possible, especially considering that $\mathcal{H}_n^d(\mathbb{C})$ is an irreducible $\mathrm{O}_n(\mathbb{C})$-module (see [2] for details), to prove that

$$(q_n^s)^{\perp} = \big\langle \mathcal{H}_n^{s+1}(\mathbb{C}) \big\rangle.$$

It has therefore been possible to determine which polynomials generate the ideals of the decompositions provided by B. Reznick.

As for the case $n = 2$, in addition to the decompositions already known for the real case, we have analyzed all possible complex decompositions and, as we expected, there is a unique representation up to an orthogonal complex transformation. This decomposition is greatly simplified by choosing another coordinates system, which provides a more uniform description of the apolar ideal. Indeed, considering the linear polynomials

$$u = y_1 + iy_2, \quad v = y_1 - iy_2,$$

from which it holds

$$\Delta = \frac{\partial^2}{\partial u\, \partial v},$$

we obtain

$$\mathcal{H}_d(\mathbb{C}) = \mathrm{span}\Big\{ u^d, v^d \Big\}.$$

Analogously, for the case of three variables, the representations of these forms appear to be more effective if we consider another system of coordinates, formed by the elements

$$u = \frac{y_1 + iy_2}{2}, \quad v = \frac{y_1 - iy_2}{2}, \quad z = y_3,$$

and in this way we can rewrite the Laplace operator as

$$\Delta = \frac{\partial^2}{\partial u \, \partial v} + \frac{\partial^2}{\partial z^2}.$$

This system also seems to be quite useful by considerations relating the representations theory (see [1]). Indeed, since $\mathcal{H}_n^d(\mathbb{C})$ is an irreducible $\mathrm{O}_n(\mathbb{C})$-module of the Lie algebra $\mathfrak{sl}_2\mathbb{C}$, which is essentially unique, we can then determine a particular basis, whose elements are obtained as eigenvectors of a specific differential operator which can be written in a quite elegant way, just using the new coordinates system.

A first analysis, trying to generalize the configurations of the first cases, focused on the arrangement of the points, which were arranged in a equirotated way on several planes. With the assistance of the Macaulay2 software, it was possible to verify the correctness of the decompositions provided by B. Reznick but unfortunately, this kind of configuration does not seem to be effective in determining suitable decompositions for the successive cases.

Despite this, the use of Macaulay2 enabled us to obtain a similar decomposition for the case $s = 5$, formed by 23 points which, however, are not all real.

As a result, since by the rank of the various components of the catalecticant map we know that

$$\mathrm{rk}(q_n^s) \geq \binom{s+2}{2},$$

the main idea, based on the information available, would be to try to analyze the possible relation

$$\mathrm{rk}(q_n^s) \stackrel{?}{=} \binom{s+2}{2} + \left\lfloor \frac{s-1}{2} \right\rfloor.$$

One way which could be considered would be to consider an ideal of points that is generated by polynomials belonging to the same orbit with respect to the action of the orthogonal group $\mathrm{O}_n(\mathbb{C})$. Indeed, this applies to cases above.

REFERENCES

[1] W. Fulton and J. Harris, *Representation theory*: *A first course*, Graduate Texts in Mathematics, vol. 129, Readings in Mathematics, Springer-Verlag, New York, 1991.

[2] R. Goodman and N. R. Wallach, *Representations and invariants of the classical groups*, Encyclopedia of Mathematics and its Applications, vol. 68, Cambridge University Press, Cambridge, 1998.

[3] A. Iarrobino and V. Kanev, *Power sums, Gorenstein algebras, and determinantal loci*, with an appendix by A. Iarrobino and S. L. Kleiman, Lecture Notes in Mathematics, vol. 1721, Springer-Verlag, Berlin, 1999.

[4] J. M. Landsberg, *Tensors*: *geometry and applications*, Graduate Studies in Mathematics, vol. 128, American Mathematical Society, Providence, RI, 2012.

[5] B. Reznick, *Sums of even powers of real linear forms*, Mem. Amer. Math. Soc. **96** (1992), no. 463.

Alma Mater Studiorum – Università di Bologna
Email address: cosimo.flavi2@unibo.it

SENSITIVITY IN CAYLEY GRAPHS

IGNACIO GARCÍA-MARCO AND KOLJA KNAUER

Abstract. In 2019, Huang proved that the sensitivity and degree of a boolean function are polynomially related, solving an outstanding foundational problem in theoretical computer science, the Sensitivity Conjecture of Nisan and Szegedy. The key point of his argument is the proof that every set of more than half the vertices of the d-dimensional hypercube Q_d induces a subgraph of maximum degree at least $\sqrt{d}$. Huang asked whether similar results can be obtained for other highly symmetric graphs.

In this work we first prove that this result cannot be extended to general Cayley graphs. We present infinite families of Cayley graphs of groups of unbounded degree that contain induced subgraphs of maximum degree 1 on more than half the vertices.

Second, we propose Coxeter groups as a suitable generalization of the hypercube with respect to Huang's question. We support our proposal with some partial results plus a large amount of computer assisted experiments.

Finally, we provide examples of cube-free Cayley graphs where every induced subgraph on more than half the vertices has high maximum degree. Interestingly, these examples rely on point-line incidence results of projective planes over a finite field.

Introduction

In [7], Nisan and Szegedy considered several measures of the complexity of a Boolean function. They proved that all these measures are polynomially related, with the sole exception of the *local sensitivity* and they conjectured that this polynomial relation should hold. More precisely, a *Boolean function* is a function $f : \{0,1\}^n \longrightarrow \{0,1\}$. The degree of f, denoted $\deg(f)$, is the degree of the only mulitilinear polynomial in $\mathbb{R}[x_1, \ldots, x_n]$ interpolating f. For $x \in \{0,1\}^n$, we denote by $x^{\{i\}} \in \{0,1\}^n$ the vector obtained by flipping the i-th position of x. The sensitivity of f at input x, denoted $s(f,x)$, equals the number of indices such that $f(x) \neq f(x^{\{i\}})$, and the *local sensitivity* is $s(f) = \max_{x\in\{0,1\}^n} s(f,x)$. In [7] they proved that $s(f) \leq 2\deg(f)^2$ and conjectured that there is a polynomial expression $p(x) \in \mathbb{R}[x]$ such that $\deg(f) \leq p(s(f))$.

Huang [5] recently proved the Sensitivity Conjecture by solving an equivalent problem proposed by Gotsmann and Linial [4]. Huang showed that an induced subgraph on more than half of the vertices of the d-dimensional hypercube Q_d has a maximum degree at least $\sqrt{d}$. For a graph $G = (V,E)$, we denote its maximum degree by $\Delta(G)$. We define the *sensitivity* $\sigma(G)$ of G as the minimum value $\Delta(K)$ among all the induced subgraphs K of G on more than $|V|/2$ vertices. With this definition Huang's result can be restated as $\sigma(Q_d) \geq \sqrt{d}$. Huang asks what can be said about $\sigma(G)$ if G is a "nice" graph with high

Both authors have been partially supported by the Spanish MICINN through grant PID2019-104844GB-I00 and by the Universidad de La Laguna through the MACACO research project.

The talk at the EACA 2022 meeting was given by the first author.

symmetry. Furthermore, since by a result of Chung et al. [2] the bound for Q_d is tight, he wonders for which graphs a tight bound on the sensitivity follows from his method.

The present work studies both of these questions by considering (simple, undirected[1], right) *Cayley graphs* of groups to be "nice" with high symmetry. That is, for a group Γ and a subset $C \subseteq \Gamma$, $\mathrm{Cay}(\Gamma, C)$ is defined as the graph with vertex set Γ and with $\{x, y\} \in E$ if and only if $x^{-1}y \in C$. First positive results in this direction were obtained by Alon and Zheng [1], who proved that $\sigma(G) \geq \sqrt{d}$ in a d-regular Cayley graph G of an elementary abelian 2-group. Recently, Potechin and Tsang [8] showed that for every d-regular Cayley graph G of an abelian group we have $\sigma(G) \geq \sqrt{d/2}$ – hence answering Huang's question. Moreover, they conjectured this lower bound holds for Cayley graphs of general groups. However shortly afterwards, Lehner and Verret [6] found a cubic Cayley graph G of a dihedral group with $\sigma(G) = 1 < \sqrt{3/2}$ – thus refuting the above conjecture. Moreover, they construct an infinite family of bipartite Cayley graphs of 2-groups of unbounded degree, with $\sigma(G) = 1$ for every member G of the family. This contributes to Huang's question since it implies that $\sigma(G)$ cannot be bounded from below by a function of the degree for general Cayley graphs. In the first part of the present work, we give two more *insensitive* families of Cayley graphs, i.e., they have unbounded degree but $\sigma(G) = 1$.

The second part of the paper concerns the question of when σ can be bounded from below in a tight way. To this end, consider the following easy consequence of Huang's result. If a Cayley graph G has a largest hypercube of dimension $\kappa(G)$ as a subgraph, then $\sigma(G) \geq \sqrt{\kappa(G)}$ (Proposition 2.1). In [2], the authors show that Huang's bound is tight for the hypercube itself, i.e., $\sigma(Q_d) = \lceil \sqrt{d} \rceil$. In the light of this result it is natural to ask when this bound is tight. We conjecture that an analogue equality holds for Coxeter groups, i.e., every Cayley graph G of a Coxeter group satisfies $\sigma(G) = \lceil \sqrt{\kappa(G)} \rceil$ (Conjecture 2.2). We provide both theoretical evidence for this conjecture proving some particular cases, and computational evidence by verifying the conjecture for small Coxeter groups. Our experimental results were obtained combining SageMath, GAP and CPLEX.

Next, we study the sensitivity of Cayley graphs in the absence of cubes, i.e., when Proposition 2.1 is useless. We show that the Levi graphs of projective planes have unbounded sensitivity (Theorem 3.1).

The results in this work are included in [3].

1. Insensitive graphs

In this section, we provide two families of Cayley graphs with unbounded degree and sensitivity equal to 1.

Let D_n denote the dihedral group of symmetries of a regular n-gon, that is, the group

$$D_n = \langle a, b \,|\, a^n = b^2 = (ab)^2 = 1 \rangle = \{1, a, \ldots, a^{n-1}, b, ab, \ldots, a^{n-1}b\}.$$

For a positive integer m, we denote by $[m]_3 \in \{1, 2\}$ the right-most nonzero entry in its representation in base 3. For example, for $m = 33$ we have that $m = 3^3 + 2 \cdot 3$ and, thus, $[m]_3 = 2$.

[1]Even if graphs are considered undirected, in figures we use arcs to represent generators of order larger than 2 to increase readability.

The following result provides a family of $(d+1)$-regular Cayley graphs with sensitivity 1 for all $d \geq 0$.

Theorem 1.1. *Let $n = 3^d$ and consider $G = \mathrm{Cay}(D_n, C)$, where $C = \{a^{3^i}b \mid 0 \leq i \leq d\} \subseteq D_n$. The set $M = \{a^i \mid [i]_3 = 1\} \cup \{a^i b \mid [i]_3 = 2\} \cup \{1, b\}$ induces a matching with $n+1$ vertices. As a consequence, $\sigma(G) = 1$.*

The *star graph* is $SG_n = \mathrm{Cay}(S_n, \{(12), (13), \ldots, (1n)\})$ (see Figure 1).

Theorem 1.2. $\sigma(SG_n) = 1$.

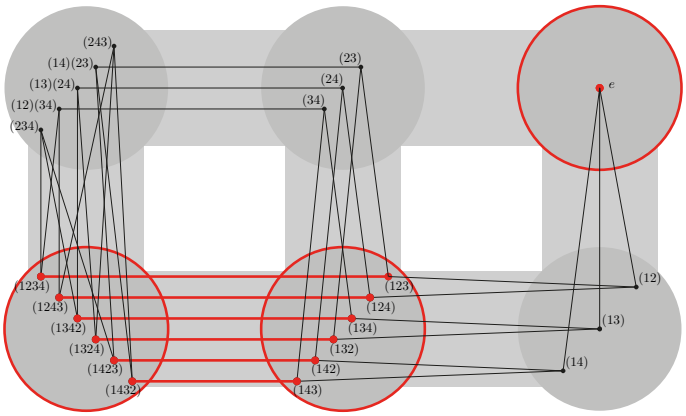


FIGURE 1. The Nauru graph SG_4. In bold, an induced subgraph with 13 vertices, a maximum degree of 1 and thus showing that $\sigma(SG_4) = 1$.

.

2. Bounds and constructions close to the hypercube

For any graph G, we denote by $\kappa(G)$ the dimension of the largest hypercube contained in G, i.e.,

$$\kappa(G) = \max\{n \in \mathbb{Z}^+ \mid Q_n \text{ is a subgraph of } G\}.$$

Proposition 2.1. *Let G be a Cayley graph, then $\sigma(G) \geq \sqrt{\kappa(G)}$.*

A finite Coxeter system is a pair (W, S), where W is a group with generators $S = \{a_1, \ldots, a_n\}$ and presentation $W = \langle a_1, \ldots, a_n \mid (a_i a_j)^{m_{ij}} = 1\rangle$ where $m_{ij} > 1$ and $m_{ii} = 2$. Coxeter classified all finite Coxeter groups as (direct products of) the members of three infinite families of increasing rank $\mathbf{A_n}, \mathbf{B_n}, \mathbf{D_n}$, one family of rank two $\mathbf{I_2}(n)$ and six exceptional groups: $\mathbf{E_6}$, $\mathbf{E_7}$, $\mathbf{E_8}$, $\mathbf{F_4}$, $\mathbf{H_3}$ and $\mathbf{H_4}$.

We have proved that $\sigma(G) = \lceil\sqrt{\kappa(G)}\rceil$ for several families of Coxeter groups including $\mathbf{A_n}$, $\mathbf{I_2}(n)$, $\mathbf{I_2}(n) \times \mathbf{I_2}(n')$ and $\mathbf{I_2}(2k_1+1) \times \ldots \times \mathbf{I_2}(2k_i+1) \times \mathbf{A_{n_1}} \times \ldots \times \mathbf{A_{n_j}}$. We have also proved that this equality is at most one unit far from being true for the groups $\mathbf{B_n}$ and $\mathbf{D_n}$. Moreover, we have verified the same equality with a computer for $\mathbf{B_3}, \mathbf{B_4}, \mathbf{D_4}, \mathbf{D_5}, \mathbf{E_6}, \mathbf{F_4}, \mathbf{H_3}$ and $\mathbf{H_4}$ among others. We believe that we have gathered together enough evidence to conjecture the following.

Conjecture 2.2. *Let G be the Cayley graph of a Coxeter group and Q_d the largest subgraph isomorphic to a cube. Then $\sigma(G) = \lceil \sqrt{\kappa(G)} \rceil$.*

3. The absence of cubes

In a sense, most of the work so far has been about Huang's lower bound (Proposition 2.1) being tight, i.e., if a bipartite Cayley graph contains a largest cube Q_d, then there is an induced subgraph of maximum degree at most $\lceil \sqrt{d} \rceil$ on more than half the vertices.

However, we do not want to give the wrong impression that this lower bound is tight in general Cayley graphs. Denote by I_q the *Levi graph*, i.e., point-line incidence graph, of the Desarguesian projective plane $P(2, q)$. It is known that I_q has no Q_d subgraphs for all $d \geq 2$. Moreover, I_q is the Cayley graph of D_{q^2+q+1} with respect to a set of $q+1$ involutions. The following thus provides a family of cube-free $(q+1)$-regular Cayley graphs and unbounded sensitivity.

Theorem 3.1. $\sigma(I_q) \geq \frac{q+1}{2} - \sqrt{q}$.

4. Conclusions

Most of the work is about Huang's lower bound (Proposition 2.1) being tight. We show that this holds for the families of graphs in Section 1, for large classes of Coxeter groups, and conjecture it for general Coxeter groups (Conjecture 2.2). We also show that Levi graphs of projective planes are cube-free graphs of unbounded sensitivity. A curiosity is that the graphs in the latter class are Cayley graphs with respect to non-minimal generating sets. It remains open whether there are Cayley graphs with respect to a minimal generating set that have bounded κ and unbounded σ.

References

[1] N. Alon and K. Zheng, *Unitary signings and induced subgraphs of Cayley graphs of $\mathbb{Z}_2^n$*, Advances in Combinatorics, 2021(1). https://doi.org/10.19086/aic.17912
[2] F. R. K. Chung, Z. Füredi, R. L. Graham, and P. Seymour, *On induced subgraphs of the cube.*, J. Comb. Theory, Ser. A, 49 (1988), pp. 180–187.
[3] I. García-Marco, K. Knauer, *On sensitivity in bipartite Cayley graphs*. J. Combin. Theory Ser. B. 154 (2022), 211-238.
[4] C. Gotsman and N. Linial, *The equivalence of two problems on the cube.*, J. Combin. Theory Ser. A, Volume 61, Issue 1 (1992), pp. 142–146.
[5] H. Huang, *Induced subgraphs of hypercubes and a proof of the sensitivity conjecture*, Ann. of Math. (2), 190 (2019), pp. 949–955.
[6] F. Lehner and G. Verret, *Counterexamples to "A conjecture on induced subgraphs of Cayley graphs"*,Ars Math. Contemp. 19 (2020): 77-82.
[7] N. Nisan and M. Szegedy, *On the degree of Boolean functions as real polynomials.*, Comput. Complexity, 4 (1994), pp. 301–313.
[8] A. Potechin and H. Y. Tsang, *A Conjecture on induced subgraphs of Cayley graphs*, arXiv:2003.13166, (2020).

Facultad de Ciencias, Universidad de La Laguna, La Laguna, Spain.
Email address: iggarcia@ull.edu.es

Departament de Matemàtiques i Informàtica, Universitat de Barcelona, Spain.
Email address: kolja.knauer@gmail.com

PRUNING ALGORITHM OF THE TAYLOR RESOLUTION - AN IMPLEMENTATION

PHILIPPE GIMENEZ AND ELVIRA PÉREZ-CALLEJO

Abstract. We propose Matlab and Singular implementations of the pruning algorithm described in [1] that starting from the Taylor resolution of a monomial ideal, return the Betti diagram of another resolution which is much smaller and sometimes minimal. The algorithm strongly depends on the way we order the monomial generators. This opens the door to studying an optimal ordering of the generators in order to reach a minimal free resolution for some families of monomial ideals.

Introduction

The study of free resolutions of monomial ideals is a very active area of research located at the interplay of Commutative Algebra, Computer Algebra and Combinatorics. The most interesting resolutions are the minimal ones, but the progress is far from complete, as they are known only for few specific families. Some non-minimal resolutions, like the Taylor [6] or the Lyubeznik [4] resolutions, are known but they provide less information and above all, they contain a lot of redundant information.

In Section 1, we introduce the concept of graded free resolution of the R-module R/I where I is a monomial ideal in a polynomial ring R in n variables over a field $\mathbb{K}$. The graded Betti numbers of R/I, and their visual display in a table, the Betti diagram, are defined as a tool to work with resolutions.

Next, in Section 2 we present the pruning algorithm described in [1] and that we have implemented in Matlab and Singular [2]. It notably reduces the redundant information in the Taylor resolution. Starting from the Taylor resolution of R/I being I a monomial ideal, and choosing an ordering on the monomials that generate I, the pruning algorithm eliminates redundant information and provides a smaller free resolution of R/I that is, sometimes, minimal. The algorithm does not require the computation of Gröbner bases, which is an advantage in terms of computational complexity.

Finally, Section 3 shows an example to illustrate our implementation. Taking the edge ideal associated with the complement of a 6-cycle and choosing an optimal pruning ordering on the monomials, we obtain the minimal free resolution of the edge ideal. This last section is also a motivation to continue researching in this direction. On the one hand, we are

The first author has been partially supported by Grant PID2019-104844GB-I00 funded by MCIN/AEI/10.13039/501100011033.

The second author has been partially supported by MCIN/AEI/10.13039/501100011033 and by "ERDF A way of making Europe", grants PGC2018-096446-B-C22 and RED2018-102583-T, by MCIN/AEI/10.13039/501100011033 and by "ESF Investing in your future", grant PRE2019-089907, as well as by Universitat Jaume I, grant UJI-B2021-02.

The talk at the EACA 2022 meeting was given by the second author.

interested in finding out which is the best pruning ordering to obtain the smallest possible resolution. On the other hand, our aim is to modify the implementation of the algorithm to solve the storage problem, which is currently an important limitation since the whole Taylor resolution must be stored before proceeding with the pruning. We would like to choose a good pruning ordering and construct the pruned resolution without storing the whole Taylor resolution.

1. Preliminaries

Let $R = \mathbb{K}[x_1, \ldots, x_n] = \bigoplus_{i\in\mathbb{N}} R_i$ be the ring of polynomials in n variables with coefficients in a field $\mathbb{K}$ with its standard grading. Let $M = \bigoplus_{i\in\mathbb{N}} M_i$ be a graded R-module. The *translated grading* on M is $M(d) = \bigoplus_{i\in\mathbb{N}} M(d)_i$ with $M(d)_i = M_{i+d}$. The element $d \in \mathbb{Z}$ is called a *shift*.

In the sequel, we will work with the R-module R/I where $I \subseteq R$ is a monomial ideal. A graded free resolution of R/I is a sequence of R-modules, all of which are free except R/I,

$$S := 0 \longrightarrow F_p \xrightarrow{\psi_p} \cdots \xrightarrow{\psi_2} F_1 \xrightarrow{\psi_1} F_0 = R \xrightarrow{\pi} R/I \xrightarrow{\epsilon} 0, \tag{1}$$

that is exact, i.e., $\mathrm{Ker}(\psi_i) = \mathrm{Im}(\psi_{i+1})$, where π is the quotient map and ψ_i is graded (of degree 0) for all i. For all i, $F_i = \bigoplus_{j\in\mathbb{N}} R(-j)^{\beta_{i,j}}$ with $\beta_{i,j} = 0$ except for a finite set of degrees j in order to have all the morphisms graded.

A graded free resolution as (1) that has the smallest possible length p, and such that all the free modules F_i have the smallest possible rank is called *minimal*. It is unique up to isomorphism. Moreover, by Hilbert's Syzygies Theorem, R/I has a minimal free resolution with a length of at most n. In a minimal free resolution of R/I, the exponents $\beta_{i,j}$ form a set of invariants of R/I known as its *graded Betti numbers*. They are usually stored in a table that contains all the numerical information of the minimal graded free resolution called the *Betti diagram* of R/I. The entry on the j-th row and i-th column of the Betti diagram is $\beta_{i,i+j}$.

Note that if we have another graded free resolution of R/I that is not minimal, e.g. the Taylor resolution as we will see later in Section 3, we can also also consider the Betti diagram of the resolution (which is no longer an invariant of the module R/I).

Given $\beta \in \mathbb{N}^n$, denote by $m^\beta = x_1^{\beta_1} \cdots x_n^{\beta_n}$ the corresponding monomial in R. Let $M = \{m^{\alpha_1}, \ldots, m^{\alpha_l}\}$ be a finite set of monomials that generate the ideal $I \subseteq R$. We will assume that M generates I minimally in order to have a unique object, but everything works without this assumption. The Taylor resolution of R/I [6] is a graded free resolution of R/I that is very easy to construct. The degree (shifts) at the i-th step of the resolution are the degrees of all the least common multiples (lcm) of subsets of M with i elements. In particular, this resolution always has l steps if $|M| = l$ and F_l has rank 1; see [3, Ex. 17.11] and [5, Section 2.2] for more details. It is in general far from being minimal.

Given a subset J of $\{1, \ldots, l\}$, we will denote by m_J the monomial $m_J = lcm\{m_j, j \in J\}$. Associated with the Taylor resolution of R/I, we have an oriented labelled graph introduced in [1] that we will call the *Taylor graph* of M and denote by $G(M)$. The vertices are the subsets of $\{1, \ldots, l\}$ and the vertex J is labelled by the monomial m_J. Moreover, for every $J \subseteq \{1, \ldots, l\}$ and every $i \in \{1, \ldots, l\} \setminus J$, there is an edge labeled by i from J to $J \cup \{i\}$.

2. Pruning algorithm

The Taylor resolution is far from being minimal. We now describe the algorithm given in [1] that starting from the Taylor resolution of R/I, prunes redundant information. The free resolution obtained is not minimal in general, but it is much smaller than other known resolutions like Taylor's or Lyubeznik's resolutions. Indeed, Lyubeznik's resolution is obtained from Taylor's via pruning [1, Algorith 3.9.].

Algorithm 2.1 ([1]). Let $M = \{m^{\alpha_i}\}_{i=1}^{l}$ be a set of generators of a monomial ideal I.

- **INPUT:** The Taylor graph of M defined in the previous section.
- **for** i **from** 1 **to** l **do**
  For all pair of vertices J and J' with an edge i from J to J', if $m_J = m_{J'}$, prune (eliminate) those two vertices and all the edges through them. **end**
- **OUTPUT:** The Betti diagram of a free resolution of R/I.

Note that in order to obtain the Betti diagram of the pruned resolution, we only need to work with integer vectors, as it has been implemented in Matlab and Singular; see [5, Apendice]. It currently follows the order of the generating monomials given by the client, but improving it and using the "best" order to find the smallest possible pruned resolution is a work in progress. The differentials in the pruned resolution could also be obtained from the pruned graph (see [1]).

3. Example

Example 3.1. Let $M = \{x_1x_4, x_3x_6, x_1x_3, x_2x_4, x_2x_5, x_1x_5, x_3x_5, x_4x_6, x_2x_6\}$ be the set of ordered generators of I, the edge ideal associated with the complement of the 6-cycle. One can load the procedure in [5, Apendice] and execute in Matlab:

```
>> complementaryCycle6v=[1 0 0 1 0 0;
     0 0 1 0 0 1;
     1 0 1 0 0 0;
     0 1 0 1 0 0;
     0 1 0 0 1 0;
     1 0 0 0 1 0;
     0 0 1 0 1 0;
     0 0 0 1 0 1;
     0 1 0 0 0 1];
>> [C,s,mcm]=TaylorResolution(complementaryCycle6v);
```

Variables `C`, `s` and `mcm` encode the Taylor graph that will be used in the next procedure. Morever, the Betti diagram of the Taylor resolution is displayed:

	0	1	2	3	4	5	6	7	8	9
−3	0	0	0	0	0	0	0	0	0	1
−2	0	0	0	0	0	0	0	0	9	0
−1	0	0	0	0	0	0	6	36	0	0
0	1	0	0	2	9	36	78	0	0	0
1	0	9	18	36	72	90	0	0	0	0
2	0	0	18	42	45	0	0	0	0	0
3	0	0	0	4	0	0	0	0	0	0
Global	1	9	36	84	126	126	84	36	9	1

The Betti diagram clearly shows that the Taylor resolution is far from being minimal. There are three rows indexed negatively and this never occurs in the Betti diagram of a minimal resolution (because the minimal degrees of syzygies strictly increase from one step to the next in a minimal resolution). Moreover, the length is $9 > 6$, the number of variables of R, which is the upper bound for the length of a minimal resolution given by Hilbert's Syzygies Theorem. The Taylor resolution of R/I has the following form:

$$0 \to R \to R^9 \to R^{36} \to R^{84} \to R^{126} \to R^{126} \to R^{84} \to R^{36} \to R^9 \to R \to R/I \to 0.$$

Now, we can load and execute the procedure where the pruning algorithm is implemented:

```
>> PruningAlgorithm(complementaryCycle6v,C,s,mcm);
```

and we obtain the Betti diagram of the pruned resolution, which is:

	0	1	2	3	4
0	1	0	0	0	0
1	0	9	16	9	0
2	0	0	0	0	1
Global	1	9	16	9	1

The pruned resolution, clearly smaller than Taylor's, is minimal.

Remark 3.2. If we choose $M' = \{x_1x_3, x_1x_4, x_1x_5, x_2x_4, x_2x_5, x_2x_6, x_3x_5, x_3x_6, x_4x_6\}$ as the ordered set of generators of the same ideal I, the Betti diagram of the pruned resolution is:

	0	1	2	3	4
0	1	0	0	0	0
1	0	9	16	9	3
2	0	0	0	3	1
Global	1	9	16	12	4

and the pruned resolution is not minimal in this case. This is a motivation for our next aim: find the "best" order of the generators for pruning.

References

[1] J. Àlvarez Montaner, O. Fernández-Ramos and P. Gimenez, Pruned cellular free resolutions of monomial ideals, *J. Algebra* **541** (2020) 126-145.

[2] W. Decker, G.-M. Greuel, G. Pfister and H. Schönemann, SINGULAR 4-3-0 — A computer algebra system for polynomial computations, 2022. Available at `www.singular.uni-kl.de`.

[3] D. Eisenbud, *Commutative Algebra with a view towards Algebraic Geometry*, Graduate Texts in Mathematics **150**, Springer, 1995.

[4] G. Lyubeznik, A new explicit finite free resolution of ideals generated by monomials in a R-sequence, *J. Pure Appl. Algebra* **51** (1988), 193–195.

[5] E. Pérez-Callejo, *Diagramas de Betti de ideales de aristas*, Universidad de Valladolid, Trabajo de Fin de Máster (in spanish), 2020. Available at `http://uvadoc.uva.es/handle/10324/43429`.

[6] D. Taylor, *Ideals generated by monomials in an R-sequence*, Chicago University, Thesis, 1966.

University of Valladolid
Email address: `pgimenez@uva.es`

Universitat Jaume I
Email address: `callejo@uji.es`

SATURATION AND VANISHING IDEALS

PHILIPPE GIMENEZ, DIEGO RUANO, AND RODRIGO SAN-JOSÉ

Abstract. We consider an homogeneous ideal I in the polynomial ring $S = \mathbb{F}_q[x_1, \ldots, x_m]$ over a finite field $\mathbb{F}_q$ and the finite set of projective rational points $\mathbb{X}$ that it defines in the projective space $\mathbb{P}^{m-1}$. We concern ourselves with the problem of computing the vanishing ideal $I(\mathbb{X})$. This is usually done by adding the equations of the projective space $I(\mathbb{P}^{m-1})$ to I and computing the radical. We give an alternative and more efficient way using the saturation with respect to the homogeneous maximal ideal.

Introduction

The aim of this work, based on [4], is to compute the vanishing ideal of a finite set of points in the projective space over a finite field. The motivation comes from Coding Theory, in which some projective codes are defined using these type of ideals. In the affine case, the computation of the vanishing ideal of a finite set of points is straightforward, but the projective case poses some additional problems. It is known that the vanishing ideal can be obtained computing the radical of a certain ideal, and we show that it can also be obtained computing the saturation with respect to the homogeneous maximal ideal, which is more efficient.

Let $\mathbb{F}_q$ be a finite field, and let $S = \mathbb{F}_q[x_1, \ldots, x_m]$ be the polynomial ring with standard grading. Let $I \subset S$ be an ideal. We denote by $X = V_{\mathbb{F}_q}(I) = \{P_1, \ldots, P_n\} \subset \mathbb{A}^m$ the finite set of rational points in which all the polynomials of I vanish. We can then consider the vanishing ideal of X, $I(X)$. With this notation we define the following evaluation map:

$$\mathrm{ev}_X : S/I(X) \to \mathbb{F}_q^n, \;\; f + I(X) \mapsto (f(P_1), \ldots, f(P_n)) \,.$$

By the definition of $I(X)$, this evaluation map is an isomorphism of $\mathbb{F}_q$-vector spaces. If we consider L a vector subspace of $S/I(X)$, we can define the *affine variety code* $C(I, L)$ as the image of L under the evaluation map ev_X. That is:

$$C(I, L) = \mathrm{ev}_X(L) = \{\mathrm{ev}_X(f + I(X)) \mid f + I(X) \in L\}.$$

In the light of this definition one may wonder how to compute the ideal $I(X)$. In this affine setting, the answer is quite straightforward. The ideal $I_q = I + \langle x_1^q - x_1, \ldots, x_m^q - x_m \rangle$

The first author has been partially supported by Grant PID2019-104844GB-I00 funded by MCIN/AEI/10.13039/501100011033.

The second author has been partially supported by Grant PGC2018-096446-B-C21 funded by MCIN/AEI/10.13039/501100011033 and "ERDF A way of making Europe", and Grant RYC-2016-20208 funded by MCIN/AEI/10.13039/501100011033 and "ESF Investing in your future".

The third author has been partially supported by Grant PID2019-104844GB-I00 funded by MCIN/AEI/10.13039/501100011033 and Grant FPU20/01311 funded by the Spanish Ministry of Universities.

The talk at the EACA 2022 meeting was given by the third author.

satisfies

$$V_{\overline{\mathbb{F}_q}}(I_q) = V_{\mathbb{F}_q}(I_q) = V_{\mathbb{F}_q}(I) = V_{\mathbb{F}_q}(I(X)) = X.$$

By Seidenberg's Lemma [8, Prop. 3.7.15], I_q is radical. Hence, in this case $I_q = I(X)$ and we obtain the vanishing ideal directly.

Following a similar idea, one can consider evaluation codes over the projective space $\mathbb{P}^{m-1}$. Let $I \subset S$ be an homogeneous ideal. Again, we consider $\mathbb{X} = V_{\mathbb{P}^{m-1}}(I) = \{[P_1], \ldots, [P_n]\} \subset \mathbb{P}^{m-1}$ the finite set of projective points defined by I with representatives P_i. Denoting the vanishing ideal of $\mathbb{X}$ by $I(\mathbb{X})$, we can define the following $\mathbb{F}_q$-linear map for each degree d:

$$\mathrm{ev}_d : S_d \to \mathbb{F}_q^n, \;\; f \mapsto \left(\frac{f(P_1)}{f_1(P_1)}, \ldots, \frac{f(P_n)}{f_n(P_n)} \right),$$

where $f_i \in S_d$ are fixed homogeneous polynomials verifying $f_i(P_i) \neq 0$. Then the image of S_d under ev_d, denoted by $C_{\mathbb{X}}(d)$, is called a *projective Reed-Muller type code* of degree d on $\mathbb{X}$. By definition, $I(\mathbb{X})_d = \ker \mathrm{ev}_d$. Thus, $S_d/I(\mathbb{X})_d \cong C_{\mathbb{X}}(d)$. It can easily be checked that the basic parameters of the code (length, dimension and minimum distance) do not depend on the choice of the polynomials f_i. These codes have been studied in various contexts [2, 3, 5].

In order to compute $I(\mathbb{X})$, as in the affine case, a natural idea would be to add the equations of the projective space to the ideal I, and check whether the resulting ideal is radical. These equations correspond to the generators of the vanishing ideal of the set of all points in $\mathbb{P}^{m-1}$ [10]:

$$I(\mathbb{P}^{m-1}) = \langle \{x_i^q x_j - x_i x_j^q, 1 \leq i < j \leq m\} \rangle.$$

We can define $I_q = I + I(\mathbb{P}^{m-1})$ and as before, if this ideal were radical, then it would be equal to $I(\mathbb{X})$. However, we have observed that this ideal is radical only in very specific cases. In general, computing the radical may be computationally intensive. It is thus an interesting problem to find an easier way to compute $I(\mathbb{X})$.

In Theorem 2.2, we prove that we can compute the vanishing ideal $I(\mathbb{X})$ using the saturation with respect to the homogeneous maximal ideal:

$$I(\mathbb{X}) = (I + I(\mathbb{P}^{m-1})) : \mathfrak{m}^{\infty}).$$

We then ask ourselves if there are many cases in which there is no need to use the saturation, i.e., $I + I(\mathbb{P}^{m-1}) = I(\mathbb{X})$. The answer is that this rarely happens, because it is equivalent to the question of whether I_q is radical or not. Following this direction, in Proposition 2.5, we show that there are finite sets of points $\mathbb{X} \subset \mathbb{P}^{m-1}$ such that there is no ideal $I \subset S$, besides $I(\mathbb{X})$, such that $I + I(\mathbb{P}^{m-1}) = I(\mathbb{X})$.

1. The vanishing ideal of a finite set of projective points

The vanishing ideal of a finite set of points satisfies many properties. We list some of them below, starting with the following lemma from [9, Cor. 6.3.19].

Lemma 1.1. *Let $[\alpha] \in \mathbb{P}^{m-1}$, with $\alpha = (\alpha_1, \ldots, \alpha_m)$, and let $I_{[\alpha]} = I(\{[\alpha]\})$ its vanishing ideal. Then*

$$I_{[\alpha]} = (\{\alpha_i x_j - \alpha_j x_i \mid 0 \leq i < j \leq m\}).$$

Corollary 1.2. *The ideal $I_{[\alpha]}$ is prime,* $\deg(S/I_{[\alpha]}) = 1$ *and* $\mathrm{ht}(I_{[\alpha]}) = m - 1$.

If we have a finite subset $\mathbb{X} \subset \mathbb{P}^{m-1}$, then

$$I(\mathbb{X}) = \bigcap_{[\beta]\in\mathbb{X}} I_{[\beta]}.$$

Taking into account that each $I_{[\beta]}$ is prime, the previous expression is an irredundant primary decomposition of $I(\mathbb{X})$.

The next result is often referred as *additivity of the degree* [7, Lem. 5.3.11].

Proposition 1.3. *Let $I \subset S$ be an homogeneous ideal and let $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_m$ be its irredundant primary decomposition. Then*

$$\deg(S/I) = \sum_{\mathrm{ht}(\mathfrak{q}_i)=\mathrm{ht}(I)} \deg(S/\mathfrak{q}_i).$$

Corollary 1.4. *Let $\mathbb{X} \subset \mathbb{P}^{m-1}$ be a finite subset. Then $\deg(S/I(\mathbb{X})) = |\mathbb{X}|$, $\mathrm{ht}(I(\mathbb{X})) = m-1$, and $S/I(\mathbb{X})$ is Cohen-Macaulay.*

2. Computing the vanishing ideal using saturation

The computation of the vanishing ideal only makes sense when $\mathbb{X} = V_{\mathbb{P}^{m-1}}(I) \neq \emptyset$. We can get $\mathbb{X} = \emptyset$ in several ways, for example, if I is 0-dimensional, or if it has positive dimension but no common zero of the homogeneous polynomials in I is in $\mathbb{P}^{m-1}$ for the corresponding field $\mathbb{F}_q$. The following lemma gives an algebraic characterization of this property.

Lemma 2.1. *Let $I \subset S$ be an homogeneous ideal. Then $\mathbb{X} = V_{\mathbb{P}^{m-1}}(I) = \emptyset$ if and only if $(I(\mathbb{P}^{m-1}) : I) = I(\mathbb{P}^{m-1})$.*

The following theorem gives a more efficient way of computing the vanishing ideal $I(\mathbb{X})$ than the usual way using the radical.

Theorem 2.2. *Let I be an homogeneous ideal such that $(I(\mathbb{P}^{m-1}) : I) \neq I(\mathbb{P}^{m-1})$. Let $\mathbb{X} = V_{\mathbb{P}^{m-1}}(I)$ and $\mathfrak{m} = (x_1, \ldots, x_m)$ the homogeneous maximal ideal. Then*

$$I(\mathbb{X}) = (I + I(\mathbb{P}^{m-1})) : \mathfrak{m}^{\infty}.$$

Example 2.3. We consider the 3-dimensional rational normal scroll defined by the equations given by the 2×2 minors of the following matrix:

$$M = \begin{pmatrix} x_0 & x_1 & x_2 & x_3 & x_4 & y_0 & y_1 & y_2 & y_3 & y_4 & z_0 & z_1 & z_2 & z_3 & z_4 \\ x_1 & x_2 & x_3 & x_4 & x_5 & y_1 & y_2 & y_3 & y_4 & y_5 & z_1 & z_2 & z_3 & z_4 & z_5 \end{pmatrix},$$

and let I be the homogeneous ideal defined by these equations. The number of rational points of this variety on $\mathbb{F}_q$ is $(q^2+q+1)(q+1)$ [2, Cor. 2.3]. We first consider the case with $q = 9$. In this situation, $|\mathbb{X}| = 910$, and the computation of the saturation with Macaulay2 [6] takes 3.65 seconds. However, the computation of the radical of I_q takes 1108.15 seconds, which shows the big difference in efficiency between the two methods.

If we consider the case $q = 11$ instead, we have $|\mathbb{X}| = 1596$. The saturation takes 5.08 seconds, and Macaulay2 [6] is not able to compute the radical of the ideal.

For this example, we have also considered Magma [1], which seems to have a well-optimized algorithm for computing the radical over fields of positive characteristic. Although the efficiency gap is reduced, the saturation is still more efficient than computing the radical.

Remark 2.4. In some cases, we can obtain the vanishing ideal using the saturation with respect to a smaller ideal. For example, if we have a polynomial $f \in S$ such that $f \notin I_{[P_i]}$, for every $[P_i] \in \mathbb{X}$, i.e., f does not vanish at any of the points of $\mathbb{X}$, then we get

$$(I_q : f^\infty) = \left(\bigcap_{[P_i]\in\mathbb{X}} (I_{[P_i]} : f^\infty) \right) \cap (Q : f^\infty) = \bigcap_{[P_i]\in\mathbb{X}} I_{[P_i]} = I(\mathbb{X}).$$

Having seen how to compute the vanishing ideal $I(\mathbb{X})$, one may wonder if there are many cases in which I_q is saturated. An equivalent question would be to ask when the equality $I + I(\mathbb{P}^{m-1}) = I(\mathbb{X})$ holds. It is easy to see that if we take $I = I(\mathbb{X})$, the vanishing ideal of a finite set of points $\mathbb{X} \subset \mathbb{P}^{m-1}$, then $I(\mathbb{X}) + I(\mathbb{P}^{m-1}) = I(\mathbb{X})$. We can also find some nontrivial examples, but in most cases we have encountered, I_q was not saturated. The next result shows that there are some finite sets of points $\mathbb{X}$ such that there are no nontrivial homogeneous ideals I with $V_{\mathbb{P}^{m-1}}(I) = \mathbb{X}$ verifying $I + I(\mathbb{P}^{m-1}) = I(\mathbb{X})$.

Proposition 2.5. *Let $\mathbb{X} \subset \mathbb{P}^{m-1}$ be a finite set of points such that the degree of the elements of a minimal generating set of $I(\mathbb{X})$ is lower than $q+1$. Then $I + I(\mathbb{P}^{m-1}) = I(\mathbb{X})$ if and only if $I = I(\mathbb{X})$.*

References

1. Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993).
2. Cícero Carvalho, Xavier Ramírez-Mondragón, Victor G. L. Neumann, and Horacio Tapia-Recillas, *Projective Reed-Muller type codes on higher dimensional scrolls*, Des. Codes Cryptogr. **87** (2019), no. 9, 2027–2042.
3. Susan M. Cooper, Alexandra Seceleanu, Ştefan O. Tohăneanu, Maria Vaz Pinto, and Rafael H. Villarreal, *Generalized minimum distance functions and algebraic invariants of Geramita ideals*, Adv. in Appl. Math. **112** (2020), 101940, 34.
4. Philippe Gimenez, Diego Ruano, and Rodrigo San-José, *Saturation and vanishing ideals*, 2022. arXiv preprint: `https://arxiv.org/abs/2202.04683`.
5. Manuel González-Sarabia, José Martínez-Bernal, Rafael H. Villarreal, and Carlos E. Vivares, *Generalized minimum distance functions*, J. Algebraic Combin. **50** (2019), no. 3, 317–346.
6. Daniel R. Grayson and Michael E. Stillman, *Macaulay2, a software system for research in algebraic geometry*, Available at `http://www.math.uiuc.edu/Macaulay2/`.
7. Gert-Martin Greuel and Gerhard Pfister, *A* **Singular** *introduction to commutative algebra*, extended ed., Springer, Berlin, 2008, With contributions by Olaf Bachmann, Christoph Lossen and Hans Schönemann.
8. Martin Kreuzer and Lorenzo Robbiano, *Computational commutative algebra. 1*, Springer-Verlag, Berlin, 2000.
9. ———, *Computational commutative algebra. 2*, Springer-Verlag, Berlin, 2005.
10. Dany-Jack Mercier and Robert Rolland, *Polynômes homogènes qui s'annulent sur l'espace projectif* $\mathrm{P}^m(\mathbf{F}_q)$, J. Pure Appl. Algebra **124** (1998), no. 1-3, 227–240.

IMUVA-Mathematics Research Institute, Universidad de Valladolid
Email address: `pgimenez@uva.es`

IMUVA-Mathematics Research Institute, Universidad de Valladolid
Email address: `diego.ruano@uva.es`

IMUVA-Mathematics Research Institute, Universidad de Valladolid
Email address: `rodrigo.san-jose@uva.es`

COMPUTATION OF CANONICAL FORMS FOR SINGLE INPUT LINEAR SYSTEMS OVER HERMITE RINGS

PHILIPPE GIMENEZ, ANDRÉS SÁEZ SCHWEDT AND TOMÁS SÁNCHEZ GIRALDA

Abstract. Let R be a commutative ring with the property that unimodular vectors can be completed to invertible matrices. Such a ring is called *Hermite* in the sense of Lam [4]. In this note we construct a canonical form for matrix pairs $(A, \underline{b})$, where $A \in R^{n\times n}$ and $\underline{b} \in R^{n\times 1}$, under the feedback equivalence relation: $(A, \underline{b})$ and $(A', \underline{b'})$ are equivalent if and only if $A' = PAP^{-1} + P\underline{b}K$ and $\underline{b'} = P\underline{b}$, for some matrices $P \in GL_n(R)$ and $K \in R^{1\times n}$.

When R is a principal ideal domain, the canonical form is easily computed by using standard Hermite and Smith normal forms. When R is a polynomial ring $K[x_1, \ldots, x_t]$, with K a field, the previously obtained canonical form remains valid, and can be determined by means of effective calculations. Our procedure consists mainly of elementary operations, combined with an adaptation of the currently available algorithms to solve the unimodular completion problem, used in the context of the Quillen-Suslin's theorem that solves Serre's conjecture.

Introduction

Throughout this paper, all rings R will be assumed to be commutative and with unit element 1. An m-input, n-dimensional linear dynamical system over a ring R, or simply a system of size (n, m) over R is a pair of matrices $\Sigma = (A, B)$ with $A \in R^{n\times n}$ and $B \in R^{n\times m}$.

Objects of this type originate in the study of linear control systems with continuous time $\underline{x'}(t) = A\underline{x}(t) + B\underline{u}(t)$, or with discrete time $\underline{x}(t+1) = A\underline{x}(t) + B\underline{u}(t)$, where $\underline{x}(t)$ is the n-dimensional vector of states, and $\underline{u}(t)$ is the m-dimensional vector of inputs. The reader is referred to [1, 2] to see the applications of this topic in Control Theory.

In this study, we will treat systems as purely algebraic objects (pairs of finite matrices with coefficients in a commutative ring).

Two systems (A, B) and (A', B') of the same size (n, m) are called *feedback equivalent* if there are invertible matrices $P \in GL_n(R)$, $Q \in GL_m(R)$ and a matrix $K \in R^{n\times m}$ such that $A' = PAP^{-1} + PBK$ and $B' = PBQ$.

We will be dealing with single-input systems, which is the case when $m = 1$. In particular, the matrix Q appearing in the definition of feedback equivalence is now of size 1×1 (i.e. a scalar q) and can be assumed to be 1, after substituting P by qP. Two single-input systems $(A, \underline{b})$ and $(A', \underline{b'})$ are therefore equivalent if $A' = PAP^{-1} + P\underline{b}K$ and $\underline{b'} = P\underline{b}$, for P, K of appropriate sizes. In this case, we say that $(\underline{A}, \underline{b})$ and $(\underline{A'}, \underline{b'})$ are equivalent via (P, K).

The first author has been partially supported by Grant PID2019-104844GB-I00 funded by MCIN/AEI/10.13039/501100011033 .

The second author has been partially supported by Grant PID2019-104844GB-I00 funded by MCIN/AEI/10.13039/501100011033 .

The talk at the EACA 2022 meeting was given by the second author.

Contents

As with many equivalence relations, some typical problems appear, e.g. the obtention of canonical forms and the determination of a complete set of invariants. The "ideal" canonical form we all dream of is the following:

$$\hat{A} = \begin{bmatrix} 0 & \cdots & 0 & 0 \\ 1 & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & 0 \end{bmatrix} \in R^{n\times n}, \qquad \hat{\underline{b}} = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \in R^{n\times 1}, \tag{1}$$

where $\hat{\underline{b}}$ is a cyclic vector for $\hat{A}$, that is to say, the $n\times n$ matrix $[\hat{\underline{b}}|\hat{A}\hat{\underline{b}}|\cdots|\hat{A}^{n-1}\hat{\underline{b}}]$ is invertible, in fact, it is the $n \times n$ identity matrix. A necessary and sufficient condition for a system $(A, \underline{b})$ to be feedback equivalent to the form (1) is the property of being *reachable* (see [2]). The system $(A, \underline{b})$ is *reachable* if the columns of the reachability matrix

$$A^*\underline{b} = [\underline{b}|A\underline{b}|\cdots|A^{n-1}\underline{b}]$$

generate R^n. For non-necessarily reachable systems, the following number associated to a system is defined. The *residual rank* of $(A, \underline{b})$ is

$$\text{res.rk}(A, \underline{b}) = \max\{i : \mathcal{U}_i(A^*\underline{b}) = R\},$$

where $\mathcal{U}_i(A^*\underline{b})$ denotes the ideal of R generated by the $i \times i$ minors of the matrix $A^*\underline{b}$, with the convention $\mathcal{U}_0(A^*\underline{b}) = R$. Reachable systems have a residual rank equal to n.

The purpose of this paper is for a single-input n-dimensional system $(A, \underline{b})$ of residual rank r, $r \geq 1$, to derive an algorithm to obtain a pseudo-canonical form with a block of size r in the form of (1). The canonical form will be explicitly constructed by means of effective calculations, for some special rings R. We refer the reader to [1, 2, 8] for further details about systems over commutative rings.

1. Theoretical solution in Hermite rings

A ring R is said to be Hermite in the sense of Lam (see [4]) if unimodular vectors can be completed to invertible matrices, or equivalently, if finitely generated stably-free R-modules are free. In particular, for every unimodular vector $\underline{b} \in R^n$ $(\mathcal{U}_1(\underline{b}) = R)$ there is an $n \times n$ invertible matrix P such that $P \cdot \underline{b}$ is the first basic vector of R^n, i.e. $\underline{b}$ is the first column of P^{-1}. The above class of rings should not be confused with Hermite rings in the sense of Kaplansky, which means that for every matrix B there is an invertible matrix P such that PB is lower triangular. Hermite (Kaplansy) implies Hermite (Lam), but the converse is not true, a counterexample is $K[x, y]$, with K a field. An example of a ring that is not even Hermite (Lam) is given in [7]. Examples of Hermite rings include all rings for which finitely generated projective modules are free, and in particular, all rings for which the Serre's conjecture is solved.

Before stating our main results, we need to define the concept of augmentation of a system. Given a single-input n-dimensional system $\Sigma = (A, \underline{b})$, we construct an $(n + 1)$-dimensional system, called its *1-augmentation*, as

$$\mathcal{A}(\Sigma) = \left(\begin{bmatrix} 0 & 0 \\ \underline{b} & A \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix} \right),$$

where the zero blocks are of appropriate sizes.

The r-augmentation of Σ is defined inductively as $\mathcal{A}^r(\Sigma) = \mathcal{A}\left(\mathcal{A}^{r-1}(\Sigma)\right)$, so that:

$$\mathcal{A}^2(\Sigma) = \left(\begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & \underline{b} & A \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \right), \ldots, \mathcal{A}^r(\Sigma) = \left(\begin{bmatrix} 0 & 0 & 0 \\ I_{r-1} & 0 & 0 \\ 0 & \underline{b} & A \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \right),$$

where I_{r-1} denotes an identity block of size $r-1$.

The main result of this section is based on the the property K_r studied in [8].

Theorem 1.1 (cf. Proposition 2.5 in [8])**.** *If R is an Hermite ring and $(A, \underline{b})$ is a single-input n-dimensional system with $res.rk(A, \underline{b}) = r$, $r \geq 1$, then we have:*

(i) $(A, \underline{b})$ is feedback equivalent to a system of the form

$$\mathcal{A}^r(A_r, \underline{b_r}) = \left(\begin{bmatrix} 0 & 0 & 0 \\ I_{r-1} & 0 & 0 \\ 0 & \underline{b_r} & A_r \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \right),$$

for some $(n-r)$-dimensional system $(A_r, \underline{b_r})$ with residual rank zero.

(ii) The feedback equivalence class of $(A, \underline{b})$ is completely determined by that of $(A_r, \underline{b_r})$. In particular, the feedback classification of n-dimensional systems of residual rank r is reduced to that of $(n-r)$-dimensional systems of residual rank 0.

From the proof of the previous theorem we extract an algorithmic procedure.

Algorithm 1.2. *Input: system $(A, \underline{b})$ with dimension n and residual rank r.*
Output: matrices P, K and an $(n-r)$-dimensional system $(A_r, \underline{b_r})$ with residual rank 0 such that $(A, \underline{b})$ is feedback equivalent to $\mathcal{A}^r(A_r, \underline{b_r})$ via (P, K).

- *If $r = 0$ then stop with output: $A_0 = A$, $\underline{b_0} = \underline{b}$, $P = I_n$ and $K = 0$.*
- *If $r \geq 1$ (i.e. $\underline{b}$ is unimodular), find P_0 such that $P_0 \cdot \underline{b} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$, and define $(A_1, \underline{b_1})$ as the corresponding blocks in $P_0 A P_0^{-1} = \begin{bmatrix} * & * \\ \underline{b_1} & A_1 \end{bmatrix}$.*
  - *If $r = 1$ then stop, output the system $(A_1, \underline{b_1})$ and the matrices (P_0, K_0), where K_0 is $-$(first row of $P_0 A P_0^{-1}$).*
  - *If $r > 1$, a recursive call to the algorithm with input $(A_1, \underline{b_1})$ and residual rank $r-1$ gives as output the system $(A'_r, \underline{b'_r})$ and the matrices (P', K').*
    Output: system $(A_r = A'_r, \underline{b_r} = \underline{b'_r})$ and matrices (P, K) given by:

$$P = \begin{bmatrix} 1 & -K'P' \\ 0 & P' \end{bmatrix} \cdot P_0, \qquad K = -(\text{first row of } PAP^{-1}).$$

2. Effective calculations in special Hermite rings

A very important step in Algorithm 1.2 is the second: given a unimodular vector $\underline{b} \in R^n$, find an $n \times n$ invertible matrix P_0 such that $P_0 \underline{b}$ is the first basic vector of R^n. Although this is theoretically possible in every Hermite ring, in practical applications we need a ring where effective computations are possible. If R is a principal ideal domain, the standard Hermite and Smith normal form algorithms solve this step. When the Hermite ring considered is $R = K[x_1, \ldots, x_t]$, with K a field, our effective calculations are performed by adapting the algorithms proposed in [3, 5, 6].

Example 2.1. We conclude with a solved example. Over the ring $R = \mathbb{Z}_2[x, y]$, consider the 3−dimensional single-input system $(A, \underline{b})$ with residual rank 2, where:

$$A = \begin{bmatrix} y^2+xy+1 & y & y \\ y^2+1 & 1 & (1+x)\,y^2+xy \\ y^2+y+x^2 & y+x & xy+1 \end{bmatrix}, \quad \underline{b} = \begin{bmatrix} 1 \\ x \\ 1 \end{bmatrix}.$$

Take $P_0 = \begin{bmatrix} 1 & 0 & 0 \\ x & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$ satisfying $P_0\underline{b} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$. Then, from $P_0AP_0^{-1}$ we extract the blocks $A_1 = \begin{bmatrix} xy+1 & (x+1)y^2 \\ x & (x+1)y+1 \end{bmatrix}$ and $\underline{b_1} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$.

Now, a recursive call to the algorithm with input $(A_1, \underline{b_1})$ yields the one-dimensional system $(A_2', \underline{b_2'}) = (y+1, x)$ with residual rank 0, together with the matrices (P', K') given by $P' = \begin{bmatrix} 1 & y \\ 0 & 1 \end{bmatrix}$ and $K' = \begin{bmatrix} 0 & 1 \end{bmatrix}$. The final output is $(A_2, \underline{b_2}) = (y+1, x)$, with matrices

$$P = \begin{bmatrix} y+x+1 & 1 & y \\ y+x & 1 & y \\ 1 & 0 & 1 \end{bmatrix}, \quad K = \begin{bmatrix} y^2+y & y^2+1 & y^2+y \end{bmatrix},$$

satisfying $PAP^{-1} + P\underline{b}K = \mathcal{A}^2(y+1, x) = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & x & y+1 \end{bmatrix}$ and $P\underline{b} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$.

References

[1] J.W. Brewer, J.W. Bunce, F.S. van Vleck, Linear Systems over Commutative Rings, Dekker, 1986.

[2] R. Bumby, E. D. Sontag, H. J. Sussmann, W. V. Vasconcelos, Remarks on the pole-shifting problem over rings, J. Pure Appl. Algebra 20 (1981), 113–127.

[3] N. Fitchas, A. Galligo, Nullstellensatz effectif et conjecture de Serre (Théorème de Quillen-Suslin) pour le calcul formel, Math. Nachr. 149 (1990), 231–253.

[4] T. Y. Lam, Serre's problem on projective modules, Springer Monographs in Mathematics, Springer, 2006.

[5] A. Logar, B. Sturmfeld, Algorithms for the Quillen-Suslin theorem, Journal of Algebra 145 (1992), 231–239.

[6] H. Lombardi, I. Yenghi, Suslin's algorithms for reduction of unimodular rows, J. Symbolic Computation 39 (2005), 707–717.

[7] D. Northcott, Finite free resolutions, Cambridge University Press, 1976.

[8] A. Sáez-Schwedt, T. Sánchez-Giralda, Coefficient assignability and a block decomposition for systems over rings, Linear Algebra Appl. 429 (2008), 1277–1287.

Philippe Gimenez, IMUVA-Mathematics Research Institute, Universidad de Valladolid. Paseo de Belén s/n, 47011 Valladolid, SPAIN.

Email address: pgimenez@uva.es

Andrés Sáez Schwedt, Departamento de Matemáticas, Universidad de León. Campus de Vegazana, 24071 León, SPAIN.

Email address: asaes@unileon.es

Tomás Sánchez Giralda, Honorary Professor, Departamento de Álgebra, Análisis Matemático, Geometría y Topología, Universidad de Valladolid. Paseo de Belén 7, 47011 Valladolid, SPAIN.

Email address: tomas.sanchez.giralda@uva.es

COMPUTING CENTRALIZERS OF THIRD ORDER OPERATORS

R. HERNÁNDEZ HEREDERO, S. L. RUEDA, AND M. A. ZURRO

Abstract. An effective computation of a basis of the nontrivial centralizer of a differential operator is the first step towards a Picard-Vessiot theory for spectral problems. A method is presented to calculate the centralizer of an order three ordinary differential operator, applying G. Wilson's results on almost-commuting operators.

1. Almost-commuting operators

Let (K, ∂) be a differential field of zero characteristic with algebraically closed field of constants $\mathbf{C}$. Let us consider an ordinary differential operator $L \in K[\partial]$ in normal form:

$$L = \partial^n + u_{n-2}\partial^{n-2} + \cdots + u_1\partial + u_0 \ . \tag{1}$$

Centralizers $\mathcal{C}(L) \subset K[\partial]$ have quotient fields that are function fields of one variable, and therefore they can be seen as affine rings of curves, and in a formal sense these are *spectral curves* [5]. In general, it is important to note that these curves may not be planar, and the basis of the centralizer $\mathcal{C}(L)$ as a $\mathbf{C}[L]$-module could have more than two generators. Given any $M \in \mathcal{C}(L)\backslash\mathbf{C}[L]$ we then have the inclusions $\mathbf{C}[L] \subset \mathbf{C}[L, M] \subseteq \mathcal{C}(L)$, and each of them could be strict. We will call L, M a *Burchnall-Chaundy (BC) pair* if the ring $\mathbf{C}[L, M]$ equals the centralizer $\mathcal{C}(L)$.

Following [6], we say that an operator A *almost commutes with* L if the operator $[L, A]$ has order $\leq n - 2$. By Proposition 2.4 in [6], we have:

(a) For each $m > 0$ there is a unique operator P_m of the form

$$P_m = \partial^m + p_{m-2}\partial^{m-2} + \cdots + p_1\partial + p_0 \ ,$$

such that P_m almost commutes with L and has the following property: *Each p_j belongs to the ring of differential polynomials $\mathbf{C}\{u_0, u_1, \ldots, u_{n-2}\}$ and is homogeneous of weight $m - j$, if we give $u_i^{(k)}$ weight $n - i + k$.*

(b) Each operator that almost commutes with L is a linear combination of the P_m's.

The first problem that arises is to calculate the family of operators $\{P_m\}_{m=1}^{\infty}$ associated with the operator L and which gives a $\mathbf{C}$ vector space of operators that almost commute with L. In [6] this family is defined as $P_m = \left(L^{m/n}\right)_+$, where $(L)^{1/n}$ is n^{th}-root of L in the local ring of pseudodifferential operators $\mathbf{C}((\partial^{-1}))$ and $(Q)_+$ stands for the differential part of a pseudodifferential operator Q.

The first author has been partially supported by Research Project PID2019-106802GB-I00 of the National Research Agency (Spain). The second author has been partially supported by UPM Research Group Modelos Matematios no Lineales. The third author has been partially supported by Grupo UCM 910444.

The talk at the EACA 2022 meeting was given by the third author.

We propose the following procedure to calculate the family of differential operators that almost commute with a given operator.

The Procedure. Given L as in (1) and a generic order m operator $P = \sum_{j=0}^{m} Y_j \partial^j$, where Y_j are differential variables over K, we obtain the commutator: $[L, P] = \sum_{s=0}^{n+m-1} F_s(Y_j, u_i)\partial^s$, where $F_s(Y_j, u_i)$ are differential polynomials in the unknowns Y_j. According to (b), solving for Y_j the differential system $\sum_{s=n-1}^{n+m-1} F_s(Y_j, u_i)\partial^s = 0$, we obtain differential polynomials $\mathbf{y}_j(u_i, C_k)$ in the u_i and integration constants C_k, $k = 1, \ldots, m+1$. Replacing Y_j by $\mathbf{y}_j(u_i, C_k)$, P becomes $\sum_{k=0}^{m} C_k P_k$ and F_s becomes

$$F_s(\mathbf{y}_j(u_i, C_k), u_i) = T_s(u_i, C_k) = \sum_{k=0}^{m} C_k T_{s,k}(u_i), s = 0, \ldots, n-2, \tag{2}$$

with commutators $[L, P_m] = T_{0,m} + T_{1,m}\partial + \cdots + T_{n-2,m}\partial^{n-2}$, for $m > 0$.

For example, applying this result to the formal operator $L_3 = \partial^3 + u_1\partial + u_0$, we can guarantee the existence of an infinite family of differential operators $\{P_m\}_{m=1}^{\infty}$ such that $[P_m, L_3]$ is an operator of order at most 1, that is

$$[P_m, L_3] = T_{0,m} + T_{1,m}\partial \ , \tag{3}$$

with $T_{0,m}$ and $T_{1,m}$ differential polynomials in the variables u_0, u_1 over K. Hence the above procedure gives the following result.

Proposition 1.1. *Let us consider an irreducible third order operator in $K[\partial]$ in normal form $L_3 = \partial^3 + u_1\partial + u_0$. The following statements are equivalent:*

(1) There is an operator M of order at most m in the centralizer $\mathcal{C}(L_3)$.

(2) The system $\sum_{k=0}^{m} T_{0,k}C_k = 0$, $\sum_{k=0}^{m} T_{1,k}C_k = 0$, can be solved for a finite set of constants $\vec{C} = \{c_k\}_{k \leq m}$, with $T_{s,k} = T_{s,k}(u_0, u_1)$ differential polynomials in u_0, u_1.

It should be noted that the system given in (2) of the previous proposition is a linear combination of the classical Boussinesq systems that we will present below.

2. The Boussinesq hierarchy and Centralizers

Next, we present the third order operators associated to classical Boussinesq systems as treated in [1], in order to effectively compute the basis $\{P_m\}_{m=1}^{\infty}$ announced in (b), to obtain equations (3). In consequence, we rewrite L_3 as

$$L_3 = \partial^3 + q_1\partial + \frac{1}{2}q_1' + q_0. \tag{4}$$

Using the notation of [1], we consider a differential recursion given by two sequences of differential polynomials $f_{n,i}, g_{n,i}$ in the ring of differential polynomials $\mathbf{C}\{u_0, u_1\}$. By direct computation we verify that:

$$Bsq_{3n+3+i} = \mathcal{R}Bsq_{3n+i}, \text{ with } Bsq_{3n+i} = \begin{pmatrix} 3\partial f_{n,i} \\ 3\partial g_{n,i} \end{pmatrix} \text{ for } i = 1, 2, \tag{5}$$

and initial conditions $(f_{0,1}, g_{0,1}) = (0, 1)$, $(f_{0,2}, g_{0,2}) = (1, 0)$, and we define the vectors:

$$v_{n+1,i} = \mathcal{R}^* v_{n,i}, \;\; v_{n,i} = \begin{pmatrix} f_{n,i} \\ g_{n,i} \end{pmatrix} \text{ and } v_{0,1} := \begin{pmatrix} 0 \\ 1 \end{pmatrix}, v_{0,2} := \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \tag{6}$$

for matrices of pseudodifferential operators:

$$\mathcal{R} = \begin{pmatrix} \mathcal{R}_1 & \mathcal{R}_2 \\ \mathcal{R}_3 & \mathcal{R}_4 \end{pmatrix} \;, \; \mathcal{R}^* = \partial^{-1}\mathcal{R}\partial = \begin{pmatrix} \partial^{-1}\mathcal{R}_1\partial & \partial^{-1}\mathcal{R}_2\partial \\ \partial^{-1}\mathcal{R}_3\partial & \partial^{-1}\mathcal{R}_4\partial \end{pmatrix} \tag{7}$$

and pseudodifferential operators:

$$\mathcal{R}_1 = 3q_0 + 2q_0'\partial^{-1}, \quad \mathcal{R}_2 = 2\partial^2 + 2q_1 + q_1'\partial^{-1}, \quad \mathcal{R}_4 = 3q_0 + q_0'\partial^{-1},$$
$$\mathcal{R}_3 = -\frac{1}{6}\partial^4 - \frac{5}{6}q_1\partial^2 - \frac{5}{4}q_1'\partial - \frac{2}{3}q_1^2 - \frac{3}{4}q_1'' + \left(-\frac{2}{3}q_1q_1' - \frac{1}{6}q_1'''\right)\partial^{-1}.$$

The systems of differential polynomials presented in (5) are called *classical Boussinesq systems* and this family is called the Boussinesq hierarchy. Let us define

$$P_{3n+i} = P_{3n-3+i}L_3 + L_{n,i} \text{ where} \tag{8}$$

$$L_{n,i} = f_{n,i}\partial^2 + \left(g_{n,i} - \frac{1}{2}\partial f_{n,i}\right)\partial + \left(\frac{1}{6}\partial^2 f_{n,i} - \partial g_{n,i} + \frac{2}{3}q_1 f_{n,i}\right). \tag{9}$$

We will call the differential operators $P_{3n+i}(u_0, u_1)$ defined in (8) the *formal Boussinesq differential operators*, and they are associated to the operator L_3 through the matrices of pseudodifferential operators $\mathcal{R}$ and $\mathcal{R}^*$. This relation will be reflected in (10).

Lemma 2.1. *For $i = 1, 2$ and $n = 1, 2, \ldots$, we have*

$$[P_{3n+i}, L_3] = T_{0,3n+i} + T_{1,3n+i}\partial, \text{ with } \begin{pmatrix} T_{0,3n+i} \\ T_{1,3n+i} \end{pmatrix} := \begin{pmatrix} \frac{1}{2}\partial & 1 \\ 1 & 0 \end{pmatrix} \cdot Bsq_{3n+i} \;. \tag{10}$$

Furthermore, fixing weights as in Section 1, (a) the differential polynomial $f_{n,i}$ is homogeneous of degree $3n + i - 2$, and $g_{n,i}$ is homogeneous of degree $3n + i - 1$.

Proof. First, observe that, by [1], (5.6), we have the formula

$$[P_{3n+i}, L] = 3\partial(f_{n+1,i})\partial + 3\left(\frac{1}{2}\partial^2(f_{n+1,i}) + \partial(g_{n+1,i})\right). \tag{11}$$

By induction on n considering (5), the equality (10) holds. On the other hand, the property on the weight of the coefficients of $f_{n,i}$ and $g_{n,i}$ can be proved by induction on n . □

Theorem 2.2. *For $i = 1, 2$ and each positive integer $n \geq 1$, the differential operator $P_{3n+i} = \partial^{3n+i} + p_{3n+i-2}\partial^{3n+i-2} + \cdots + p_1\partial + p_0$ satisfies: Each coefficient p_j is homogeneous of weight $3n + i - j$, if we give $u_i^{(k)}$ weight $3 - i + k$, $i = 1, 2$. In addition, the following equality of differential operators is fulfilled:*

$$P_{3n+i} = \left(L_3^{(3n+i)/3}\right)_+ \;. \tag{12}$$

Proof. We will proceed by induction on n. From (8), (9) and Lemma 2.1, the operator P_{3n+i} has the required weighed coefficients. By (11), P_{3n+i} and L almost commute. Wilson's result on the uniqueness of the almost commuting basis, Section 1, (a) implies (12). □

We will use the family of operators that almost commute with L_3 to build a basis for its centralizer. Whenever the centralizer of L in $K[\partial]$ is non-trivial, i.e. $\mathcal{C}(L) \neq \mathbf{C}[L]$, the results of K. Goodearl in [2] allow the description of a basis of $\mathcal{C}(L)$ as a $\mathbf{C}[L]$-module. In particular, by [2], Theorem 1.2, we know that the rank of $\mathcal{C}(L_3)$ as a free $\mathbf{C}[L_3]$-module is a divisor of 3. There therefore are only two options, either the rank is 1 and then $\mathcal{C}(L_3)$ is trivial $\mathcal{C}(L_3) = \mathbf{C}[L_3]$, or the rank is 3 and then $\mathcal{C}(L_3) = \mathbf{C}[L_3, A_1, A_2]$, where A_i is an operator of order congruent with i mod 3, and they have minimal order for this property. We would like to emphasize that the key fact is to decide whether $\mathcal{C}(L_3)$ is non-trivial or even better, determine L_3 such that $\mathcal{C}(L_3)$ is non-trivial. This is precisely the purpose of this work.

Theorem 2.3. *Let $L = \partial^3 + \tilde{u}_1\partial + \tilde{u}_0$ be an operator such that $(\tilde{u}_0, \tilde{u}_1)$ satisfies one of the Boussinesq systems defined in* (5)*. Then L has a nontrivial centralizer in $K[\partial]$ that equals the free $\mathbf{C}[L]$-module of rank 3 with basis $\{1, A_1, A_2\}$, with $A_i = P_{3n_i+i}(\tilde{u}_0, \tilde{u}_1, \tilde{\mathbf{c}}_i)$ of minimal order $3n_i + i$, $i = 1, 2$ and $n_i \geq 0$ and $\tilde{\mathbf{c}}_i \in \mathbf{C}^{n_i+1}$.*

Proof. By Lemma 2.1, $P_{3n_i+i}(\tilde{u}_0, \tilde{u}_1, \tilde{\mathbf{c}}_i)$ belongs to the centralizer. In addition, we know that the rank of $\mathcal{C}(L)$ as a free $\mathbf{C}[L]$-module equals 3, thus its basis must be $\{1, A_1, A_2\}$, with A_i as defined above. □

As a consequence of theorems 2.2 and 2.3, we conclude that the basis of the centralizer $\mathcal{C}(L)$ can be computed by means of the procedure described in Section 1. To illustrate our results, we perform our methods on $L = \partial^3 - \frac{6}{x^2}\partial + \frac{12}{x^3} + h$, with $h \neq 0$, to obtain $A_1 = \partial^4 - \frac{8}{x^2}\partial^2 + \frac{24}{x^3}\partial - \frac{24}{x^4}$ and $A_2 = \partial^5 - \frac{10}{x^2}\partial^3 + \frac{40}{x^3}\partial^2 - \frac{80}{x^4}\partial + \frac{80}{x^5}$ in notations of 2.3. An effective computation of the basis of the centralizer is the first step towards an effective Picard-Vessiot theory for spectral problems iniciated in [3] and [4] for second order operators.

References

[1] R. Dickson, F. Gesztesy, and K. Unterkofler, *A new approach to the boussinesq hierarchy*, Math. Nachr. **198** (1999), 51–108.

[2] K.R. Goodearl, *Centralizers in differential, pseudo-differential and fractional differential operator rings*, Rocky Mountain Journal of Mathematics **13** (1983), no. 4, 573–618.

[3] J. J. Morales-Ruiz, S.L. Rueda, and M.A. Zurro, *Factorization of KdV Schrödinger operators using differential subresultants*, Adv. Appl. Math. **120** (2020), 102065.

[4] ———, *Spectral Picard–Vessiot fields for Algebro-geometric SchrÖdinger operators*, Annales de l'Institut Fourier **71** (2021), no. 3, 1287–1324.

[5] E. Previato, S. L. Rueda, and M. A. Zurro, *Commuting Ordinary Differential Operators and the Dixmier Test*, "SIGMA (Symmetry, Integrability and Geometry: Methods and Application)" **15** (2019), no. 101, 23 pp.

[6] G. Wilson, *Algebraic curves and soliton equations*, Geometry Today, 1985, pp. 303–329.

Universidad Politécnica de Madrid
Email address: rafael.hernandez.heredero@upm.es

Universidad Politécnica de Madrid
Email address: sonialuisa.rueda@upm.es

Universidad Autónoma de Madrid
Email address: mangeles.zurro@uam.es

SEMI-SUPERVISED MACHINE LEARNING: A HOMOLOGICAL APPROACH

ADRIÁN INÉS, CÉSAR DOMÍNGUEZ, JÓNATHAN HERAS, GADEA MATA AND JULIO RUBIO

ABSTRACT. In this paper we describe the mathematical foundations of a new approach to semi-supervised Machine Learning. Using techniques of Symbolic Computation and Computer Algebra, we apply the concept of *persistent homology* to obtain a new semi-supervised learning method.

INTRODUCTION

Machine Learning and Deep Learning methods have become the state-of-the-art approach for solving data classification tasks. In order to use those methods, it is necessary to acquire and label a considerable amount of data; however, this is not straightforward in some fields, since data annotation is time consuming and may require expert knowledge. This challenge can be tackled by means of semi-supervised learning methods that take advantage of both labelled and unlabelled data. In our team we have applied this Machine Learning paradigm in various applied projects (e.g. [3]). In this paper, we present a new semi-supervised learning method based on techniques from Topological Data Analysis. In particular, we have used a homological approach that consists of studying the persistence diagrams associated with data from binary classification tasks using the bottleneck and Wasserstein distances. In addition, we have carried out a thorough analysis of the developed method using 5 structured datasets. The results show that the semi-supervised method developed in this work outperforms both the results obtained with models trained with only manually labelled data, and those obtained with classical semi-supervised learning methods, improving the models by up to a 16%.

1. CONCEPTUAL PRESENTATION

Our method falls within the discipline of Topological Data Analysis (hereinafter TDA), a field devoted to extracting topological and geometrical information from data. And the problem undertaken is motivated by the challenge of obtaining enough annotated data to apply Machine Learning techniques. To that end, a family of methods that has been successfully applied in the literature is semi-supervised learning. Semi-supervised learning methods provide a means of using unlabelled data to improve models' performance when we have access to a large corpus of data that is difficult to annotate. Traditional semi-supervised learning algorithms, such as Label Spreading [4] and Label Propagation [5], focus on the distance among the data points to annotate unlabelled data points; i.e. on the metric and density characteristics of the data in a dataset. However, there are contexts where metric approaches could be misleading. As shown in Figure 1, distances are not the right discriminators in complex situations and, therefore other ideas are needed. Our inspiration comes from the *Manifold Hypothesis* [2], which explores when high dimensional data could tend to lie in low dimensional manifolds. Roughly speaking, our method works under the hypothesis that each

This work was partially supported by the projects PID2020-115225RB-I00 and PID2020-116641GB-I00, funded by MCIN/AEI/10.13039/501100011033 and by "European Union NextGenerationEU/PRTR".

Contents

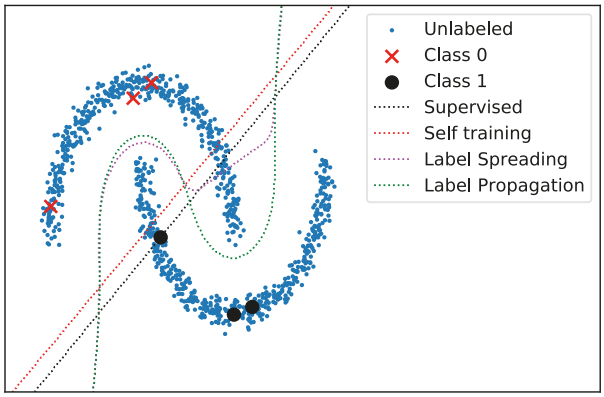


FIGURE 1. Example with two "connected manifolds"

class in the dataset lies on a manifold. In particular, homological information should be respected when we add an unlabelled point to one of the classes. Our method is therefore as follows: given two sets of data points A and B, corresponding to the points labelled with class 1 and class 2, respectively, we assume there are two manifolds associated with each set, $\mathcal{M}_A$ and $\mathcal{M}_B$ respectively; now, given an unlabelled data point x, if x belongs to class 1, for instance, then $A \cup \{x\}$ would lie on a manifold more similar to $\mathcal{M}_A$ than the manifold corresponding to $B \cup \{x\}$ with respect to $\mathcal{M}_B$.

All the code developed for this project and also the conducted experiments are available at the project webpage `https://github.com/adines/TTASSL`.

2. DESCRIPTION OF THE METHOD

In this section, we describe the semi-supervised learning algorithm that we have designed to tackle binary classification tasks. We start with a set X_1 of points from class 1, a set X_2 of points from class 2, and a set X of unlabelled points. The objective of our algorithms is to annotate the elements of X by using topological properties of X_1 and X_2. We assume some familiarity with notions employed in TDA such as Vietoris-Rips filtration (we denote the Vietoris-Rips filtration associated with a set X by V_X), persistence diagrams (we denote the persistence diagram associated with a filtration F by $P(F)$), and the bottleneck and Wasserstein distances (denoted by d_B and d_W respectively). For a detailed introduction to these topics see [6].

Our semi-supervised learning algorithm takes as input the sets X_1 and X_2, a point $x \in X$, a threshold value t, and a flag that indicates whether the bottleneck or the Wasserstein distance should be used. We denote the chosen distance as d. The output produced by our algorithm is whether the point x belongs to X_1, X_2 or none of them. In order to decide the output of the algorithm, our hypothesis is that if a point belongs to X_1, analogously for X_2, then when adding the point to the

manifold on which X_1 lies, the topological variation will be minimal; whereas if the point does not belong to X_1, the variation will be greater. In particular, we proceed as follows:

(1) Construct the Vietoris-Rips filtrations V_{X_1}, V_{X_2}, $V_{X_1\cup\{x\}}$ and $V_{X_2\cup\{x\}}$;
(2) Construct the persistence diagrams $P(V_{X_1})$, $P(V_{X_2})$, $P(V_{X_1\cup\{x\}})$ and $P(V_{X_2\cup\{x\}})$;
(3) Compute the distances $d(P(V_{X_1}), P(V_{X_1\cup\{x\}}))$ and $d(P(V_{X_2}), P(V_{X_2\cup\{x\}}))$, from now on d_1 and d_2 respectively;
(4) If both d_1 and d_2 are greater than the threshold t, return none; otherwise, return the set associated with the minimum of the distances d_1 and d_2.

The algorithm above is diagrammatically described in Figure 2, and it is applied to all the points of the set of unlabelled points X.

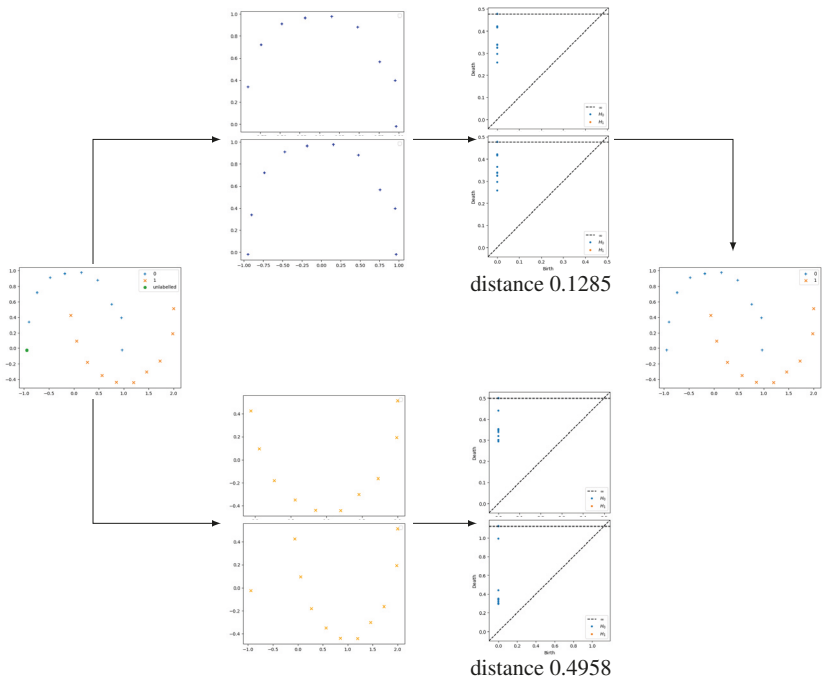


FIGURE 2. Example of the application of our method using the bottleneck distance, and using 0.6 as threshold value.

3. EVALUATION

Table 1 presents the results with 5 different datasets taken from the UCI Machine Learning Repository [1], training the models with two machine learning algorithms, which are Support Vector Machines (SVM in the table) and Random Forest (RF), and comparing our method with three classical semi-supervised learning techniques (namely, Label Propagation [5], Label Spreading [4],

TABLE 1. Accuracy results for the SVM and RF classifiers trained with data annotated for each of the annotation methods (classical and homological) together with the results obtained with the initial data (base) in the 5 structured datasets. The best result for each dataset is highlighted in bold face.

Method	Banknote		Breast Cancer		Ionosphere		Prima Indian		Sonar		Mean (std)	
	SVM	RF	SVM	RF	SVM	RF	SVM	RF	SVM	RF	SVM	RF
Base	97.0	88.6	89.3	**96.1**	80.0	93.3	65.7	60.8	61.3	64.5	78.7(15.2)	80.7(16.7)
Label Propagation	97.4	93.2	90.3	89.3	86.7	86.7	64.3	68.5	58.1	54.8	79.3(17.1)	78.5(16.3)
Label Spreading	97.4	93.2	90.3	89.3	86.7	86.7	64.3	68.5	58.1	54.8	79.3(17.1)	78.5(16.3)
Self Training classifier	95.1	93.6	35.9	35.9	85.0	86.7	66.4	66.4	58.1	67.7	68.1(23.2)	70.1(22.4)
Bottleneck threshold 0.8	**99.2**	92.4	93.2	91.3	78.3	**95.0**	63.6	64.3	61.3	64.5	79.1(17.0)	**81.5(15.6)**
Bottleneck threshold 0.6	**99.2**	91.3	89.3	90.3	75.0	88.3	59.4	63.6	48.4	45.2	74.3(20.9)	75.7(20.6)
Bottleneck threshold 0.4	97.4	90.5	87.4	85.4	78.3	86.7	63.6	62.9	45.2	45.2	74.4(20.5)	74.1(19.5)
Bottleneck threshold 0.2	97.4	90.5	87.4	85.4	78.3	86.7	63.6	62.9	45.2	45.2	74.4(20.5)	74.1(19.5)
Bottleneck threshold 0.0	97.4	90.5	87.4	85.4	78.3	86.7	63.6	62.9	45.2	45.2	77.1(22.6)	74.1(19.5)
Wasserstein threshold 0.8	97.4	89.8	92.2	88.4	80.0	**95.0**	**68.5**	67.8	61.3	64.5	79.9(15.3)	81.1(13.9)
Wasserstein threshold 0.6	**99.2**	93.6	89.3	87.4	70.0	91.7	61.5	61.5	**74.2**	61.3	78.9(15.2)	79.1(16.3)
Wasserstein threshold 0.4	97.0	96.2	87.4	87.4	76.7	81.7	60.8	62.9	71.0	71.0	78.6(14.1)	79.8(13.2)
Wasserstein threshold 0.2	97.0	96.2	87.4	87.4	76.7	81.7	60.8	62.9	71.0	71.0	78.6(14.1)	79.8(13.2)
Wasserstein threshold 0.0	97.0	96.2	87.4	87.4	76.7	81.7	60.8	62.9	71.0	71.0	78.6(14.1)	79.8(13.2)

and Self Training) to annotate the unlabelled data. From these results, we can extract several conclusions: our method improves the base results in 8 out of the 10 models and obtains better results than the classical semi-supervised learning techniques in 8 out of the 10 models.

4. CONCLUSIONS AND FURTHER WORK

In this paper, we have studied the application of Topological Data Analysis techniques to the semi-supervised learning setting. The results show that our method can create classification models that achieve better results than those obtained when using classical semi-supervised learning methods. We plan to extend our work in different ways. First of all, the proposed method can be expanded to multi-class classification tasks, and, an iterative version of the algorithm can be easily developed. In addition, we plan to design new semi-supervised learning algorithms based on other notions from TDA, taking further advantage of the *Manifold Hypothesis*.

REFERENCES

[1] D. Dua and C. Graff. *UCI Machine Learning Repository*. `http://archive.ics.uci.edu/ml`. 2017

[2] C. Fefferman, S. Mitter and H. Narayanan. *Testing the Manifold Hypothesis*. Journal of the American Mathematical Society. Vol. 29 (4), 983–1049. 2016

[3] A. Inés, C. Domínguez, J. Heras, E. Mata, and V. Pascual. *Biomedical image classification made easier thanks to transfer and semi-supervised learning*. Computer Methods and Programs in Biomedicine. Vol. 198, 105782. 2021

[4] D. Zhou, O. Bousquet, T. N. Lal, J. Weston and B. Schölkopf. *Learning with local and global consistency*. Advances in Neural Information Processing Systems 16, 321–328. 2004

[5] X. Zhu and Z. Ghahramani. *Learning from Labeled and Unlabeled Data with Label Propagation*. Tech. Report. 2002

[6] A. Zomorodian. *Topological data analysis*. Advances in Applied and Computational Topology. Vol. 70, 1–39. 2012

Departamento de Matemáticas y Computación. Universidad de La Rioja
Email address: `{adrian.ines, cesar.dominguez, jonathan.heras}@unirioja.es`
Email address: `{gadea.mata, julio.rubio}@unirioja.es`

DEALING WITH DEGENERACIES IN AUTOMATED THEOREM PROVING IN GEOMETRY: A ZERO-DIMENSIONAL APPROACH

ZOLTÁN KOVÁCS, TOMÁS RECIO, LUIS F. TABERA, AND M. PILAR VÉLEZ

Abstract. In the presentation we will start by reporting, using various examples to present the current development in GeoGebra of geometric automated reasoning tools by means of computational algebraic geometry algorithms. We will then introduce and analyze the case of the degeneracy conditions that so often arise in the automated deduction in geometry context, proposing two different ways for dealing with them. The first is to work with the saturation of the hypotheses ideal with respect to the ring of geometrically independent variables, as a way to globally handle the statement over all non-degenerate components. The second is to consider the reformulation of the given hypotheses ideal considering the independent variables as invertible parameters, exploiting the specific properties of this zero-dimensional case to analyze the truth of the statement over each non-degenerate component.

Introduction

This presentation deals with the mathematical and technological issues involved in our current development of a *mechanical geometer*, built on top of GeoGebra, a free, dynamic mathematics system, available on and offline, in various devices (computer, laptops, tablets, smartphones), with more than 100 million users all over the world (see `http://www.geogebra.org`).

In our presentation we will use a series of examples to illustrate the current performance and ongoing development, of automated reasoning tools in GeoGebra, and its algebraic geometry background. Then we reflect on some (unexpected for a standard user) problems that might arise, due to the interaction of the different steps involved in the process, such as the user's specific interpretation and introduction of the geometric statement, the internal algebraic translation, the algorithmic manipulation of polynomial ideals towards the final output (and again, its interpretation by the user). This somewhat confusing panorama: intuitive algebraic formulation, manipulation and derivation of geometric facts vs (sometimes) contradictory GeoGebra's output, is merely a warning of the need to revise our approach. Specifically, in this presentation we will focus on a particular kind of such problems, the unexpected degenerate instances appearing in the hypotheses. Some solutions to accomplish this problem have recently been published by the authors in [KRTV(2021)], https://doi.org/10.3390/math9161964.

The authors have been partially supported by a grant PID2020-113192GB-I00 (Mathematical Visualization: Foundations, Algorithms and Applications) from the Spanish MICINN.

The talk at the EACA 2022 meeting was been given by the fourth author.

1. Algebraic formulation

Roughly speaking, the mathematics behind the mechanical geometer involve the translation of the geometric facts into a collection of polynomial equations and inequalities, and the corresponding manipulation by means of (complex or real) computational algebraic geometry algorithms developed by the authors (see [RV(1999), KRV(2019)]), involving the Hilbert dimension, ideal elimination and saturation computations using the free computer algebra software Giac (see [KP(2015)], embedded in GeoGebra for Gröbner Bases computations and some freely available tools for Cylindrical Algebraic Decomposition in the real case [AVRK(2019)].

2. Dealing with degeneracy

One of the more frequent outputs of the automated reasoning tools is the inclusion of a list of degenerate cases (e.g. circles with a radius of zero, triangles collapsing to a line, etc.) in the answer to the automated reasoning tools. Cases that have to be avoided for the generic truth of a certain statement. This problem has long been well-known, even in quite simple cases (see [RV(1999)]), and see [LPR(2020)] for a more systematic study.

In order to avoid these situations as much as possible, the algorithm in [RV(1999)], quite successfully implemented in GeoGebra (see [BHJKPRW(2015)], [KRV(2018)]), considers as "generally true" those statements where the thesis vanishes over all the irreducible components of the hypothesis variety describing all the non-degenerate instances; i.e. it disregards as irrelevant the fact that the thesis fails over the components that include degenerate cases. Likewise, a statement is labeled as "generally false" if the thesis does not vanish identically for every non-degenerate irreducible component of the hypotheses variety, those describing the non-degenerate instances; it does not matter that the thesis holds for the components that include degenerate cases. It therefore turns out that the key concept is that of "degeneracy".

The usual approach to dealing with this issue is, first, to consider that the different steps of a construction provide a collection of points that rule the construction, i.e. if they are dragged along the window of the application, the whole construction should follow them. Second, the truth or falsity of geometry statements is checked by eliminating all variables except the free ones in an ideal involving hypotheses and thesis (see [RV(1999), KRV(2019)]).

The algebraic translation of this concept of "freedom" is related first to the consideration of the coordinates of the points as variables in the polynomial ring describing the geometric statement. The counterpart for the idea of a free or semi-free point is therefore the concept of a set of independent variables with respect to an ideal: a set of variables such that the given ideal does not include any polynomial constraint among them, so they are free. Algorithmically, we are talking about variables such that the elimination of the remaining variables in the ideal yields the zero ideal. Finally, the fact that these free variables "rule" the construction can be thought of as referring to a set of variables so that the remaining ones are finitely determined by the free ones: a maximal set of independent variables. Unfortunately, this condition does not necessarily imply that the cardinal of this maximal set is also maximum among the possible collections of sets of independent variables; i.e. it can be less than the Krull dimension (also known as the Hilbert dimension) of the given ideal.

To deal with this context, the elimination algorithm implemented in GeoGebra automatically associated – following the construction steps – a maximal set of algebraically independent variables to the hypotheses ideal H, and considers as "degenerate" *those irreducible components of $V(H)$ where these variables do not remain independent, but constrained by some relations*. Then, as already defined above, it declares a statement to be generally true (respectively, generally false) iff it is true (false) for all the non-degenerate components.

Let us consider K and L to be fields, with L an algebraically closed extension on K (for instance $L = C$ and $K = Q$), and an algebraically translated statement $\{H \Rightarrow T\}$. Let $H = \langle h_1, \ldots, h_r \rangle$ and $T = \langle f \rangle$ be the hypotheses and thesis ideals in the polynomial ring $K[X]$, where the variables $X = \{x_1, \ldots, x_n\}$ refer to the symbolic coordinates involved in the algebraic description of the hypotheses in K^n. Take the algebraic variety $V(H)$ (respectively, $V(T)$) in the affine space L^n defined over K. Next, following a geometric intuition or through the steps of the geometric construction in the Dynamic Geometry program, fix a maximal set $Y = \{x_1, \ldots, x_d\}$ of independent variables for the hypotheses ideal H and denote by $Z = \{x_{d+1}, \ldots, x_n\}$ the remaining variables.

A practical alternative, without assuming that d is the Hilbert dimension of H, is proposed in [KRTV(2021)] and outlined below.

Definition 2.1. We say that a primary component of H, or an irreducible component of $V(H)$, is non-degenerate iff Y remains independent over the primary component, i.e., if there is no polynomial in the Y variables that vanishes over all the corresponding irreducible component.

Remark 2.2. Note that the current definition is similar to the one in [RV(1999)], but now we do not require the dimension of H to be equal to the cardinal of the set of variables -a quite small advantage, but useful in practice. Moreover, following the consideration in the last paragraph of the previous section, we assume for the rest of the paper that non-degenerate components have a dimension d, although d does not have to be the dimension of H.

Now let us collect different algorithmic criteria for generally true or false statements.

Proposition 2.3. *The statement $\{H \Rightarrow T\}$ is* generally true *if and only if*

$$\langle h_1, \ldots, h_r, f \cdot t - 1 \rangle \, K[X,t] \cap K[Y] \neq \langle 0 \rangle \, .$$

Proposition 2.4. *The statement $\{H \Rightarrow T\}$ is* generally false *if*

$$\langle h_1, \ldots, h_r, f \rangle \, K[X] \cap K[Y] \neq \langle 0 \rangle \, .$$

And adding the condition $dim(H) = d$, this inequation holds if the statement is generally false.

Statements that are neither generally true nor generally false are called "true on parts, false on parts" or "true on components". These results show the interest of addressing two further issues:

- How to fully verify the *generally false* case when $dim(H) \neq d$. See Example 2 in [KRV(2019)], where the zero elimination requirement derived from Proposition 2 is necessary but not sufficient for being not generally false.
- How to discriminate non-degenerate components where the thesis holds from those where the thesis fails, in the "true on components" case. This is usually a source

of geometric insight, as it shows further restrictions that have to be added for a certain statement to be true, usually related to the lack of precision of the algebraic translation.

Of course, an immediate solution could be to compute the primary decomposition of H and then for each component, to verify if it is non-degenerate, by eliminating all variables except Y; by definition, the output should be zero iff the component is non-degenerate. Then, for each non-degenerate component, as they are of dimension d, by our assumption, we could fully apply the criterion expressed in the above propositions. However, obtaining a complete primary decomposition is usually quite challenging on a personal computer when using a standard computer algebra program. In our presentation we will develop a much more practical alternative without assuming that d is the Hilbert dimension of H, that is, as proposed in [KRTV(2021)]:

1) isolating the collection of non-degenerate components of H by means of *saturation*, and then applying the usual elimination criteria.
2) working directly in a zero-dimensional context, extending the ideal H to the ring $K(Y)[Z]$, i.e. including the selected free variables as elements of the coefficient field.

We refer to [KRTV(2021)] for details and examples of the performance of both approaches.

References

[AVRK(2019)] Abar, C. ; Vajda, R.; Recio T.; Kovács, Z. Conectando Mathematica e GeoGebra para explorar construçoes geométricas planas, Brazilian Wolfram Technology Conference 2019,https://tinyurl.com/geogebra-real-art.

[BHJKPRW(2015)] Botana; F., Hohenwarter, M. ; Janičić, P.; Kovács, Z.; Petrović, I.; Recio, T.; Weitzhofer, S. Automated Theorem Proving in GeoGebra: Current Achievements. *Journal of Automated Reasoning* **2015**, *55*(1), 39–59.

[KRV(2018)] Kovács, Z. ; Recio, T.; Vélez, M. P. Using Automated Reasoning Tools in GeoGebra in the Teaching and Learning of Proving in Geometry. *International Journal for Technology in Mathematics Education* **2018**, *25*(2), 33–50.

[KP(2015)] Kovács, Z. ; Parisse, B. Giac and GeoGebra: Improved Gröbner Basis Computations, In: Gutierrez, J., Schicho, J., Weimann, M. (eds.) Computer Algebra and Polynomials. Lecture Notes in Computer Science, 8942, Springer International Publishing **2015.**

[KRTV(2021)] Kovács, Z. ; Recio, T.; Tabera, L. F. ; Vélez, M. P. Dealing with Degeneracies in Automated Theorem Proving in Geometry. *Mathematics* **2021**, 9, 1964. https://doi.org/10.3390/math9161964

[KRV(2019)] Kovács, Z. ; Recio, T.; Vélez, M. P. Detecting truth, just on parts. *Revista Matemática Complutense* **2019**, *32*(2), 451–474.

[LPR(2020)] Ladra, M. ; Páez-Guillán, P.; Recio, T. Dealing with negative conditions in automated proving: tools and challenges. The unexpected consequences of Rabinowitsch's trick. *Revista de la Real Academia de Ciencias Exactas, Físicas y Naturales* **2020**, *114*(4).

[RV(1999)] Recio, T. ; Vélez, M. P. Automatic Discovery of Theorems in Elementary Geometry. *Journal of Automated Reasoning* **1999**, *23*, 63–82.

The Private University College of Education of the Diocese of Linz, Austria
Email address: zoltan@geogebra.com

Universidad Antonio de Nebrija, Madrid, Spain
Email address: trecio@nebrija.es
Email address: pvelez@nebrija.es

Universidad de Cantabria, Santander, Spain
Email address: taberalf@unican.es

SOME OPTIMAL (r, δ)-LOCALLY RECOVERABLE CODES

H. MARTÍN-CRUZ

ABSTRACT. We give several families of optimal (r, δ)-locally recoverable codes. Most of the constructions of these codes are new, and they are designed for repairing one position by accessing at most r positions but tolerating other $\delta - 1$ erasures. These results were obtained jointly with C. Galindo and F. Hernando.

INTRODUCTION

Locally recoverable codes arose in [5] to treat the repair problem for large scale distributed and cloud storage systems. This problem consists of recovering the information of a failing node from the others. A locally recoverable code with locality r, C, is an error-correcting code such that any position in C can be recovered from at most r other positions of C. There are many papers on this type of codes, see for instance [12, 6, 7, 11]. An improvement are (r, δ)-locally recoverable codes (Definition 1.1), introduced in [9], and designed for simultaneous multiple device failures. They admit a Singleton-like bound (see Proposition 1.2). Optimal (r, δ)-locally recoverable codes are those achieving that bound and they have been studied in [2, 1, 3, 10].

In this paper, we discuss some of the results accomplished with C. Galindo and F. Hernando, which will be published somewhere, together with their proof. Our main goal is to provide several families of optimal (r, δ)-locally recoverable codes (Theorems 3.1 and 3.2).

1. LOCALLY RECOVERABLE CODES WITH LOCALITY (r, δ)

From now on, q is a prime power and $\mathbb{F}_q$ the finite field with q elements. Let C be a linear code over $\mathbb{F}_q$ with parameters $[m, k, d]_q$.

Definition 1.1. A code C as above is an (r, δ)-locally recoverable code (or a locally recoverable code with locality (r, δ)) if for any position j, $1 \leq j \leq m$, there is a set $\overline{R} = \overline{R}(j) \subseteq \{1, \ldots, m\}$ of positions such that:

(1) $\#\overline{R} \leq r + \delta - 1$ and $j \in \overline{R}$; and
(2) $\mathrm{d}(C[\overline{R}]) \geq \delta$,

where $C[\cdot]$ denotes the punctured code. The original definition of code with locality r corresponds to the case $\delta = 2$ and condition (2) means that an erasure at position j plus any other $\delta - 2$ erasures in $\overline{R} \backslash \{j\}$ can be corrected by using the remaining r positions.

Next, we state the before mentioned Singleton-like bound:

The author has been partially supported by MCIN/AEI/10.13039/501100011033 and by "ERDF A way of making Europe", grant PGC2018-096446-B-C22, as well as by Universitat Jaume I, grants UJI-B2021-02 and PREDOC/2020/39.

Proposition 1.2. [9] *The inequality*

$$k + d + \left(\left\lceil \frac{k}{r} \right\rceil - 1 \right) (\delta - 1) \leq m + 1$$

holds for the parameters $[m, k, d]_q$ of any (r, δ)-locally recoverable code C. C is called an optimal (r, δ)-locally recoverable code (or simply, an optimal code) when one gets equality.

2. Our supporting codes

Let $n \geq 2$ be a positive integer. For each $i = 1, \ldots, n$, pick a non-empty subset S_i of $\mathbb{F}_q$ of cardinality $m_i \geq 2$. Set

$$S = S_1 \times \cdots \times S_n = \{\boldsymbol{\gamma}_1, \ldots, \boldsymbol{\gamma}_m\} \subseteq \mathbb{F}_q^n.$$

The ideal of $\mathbb{F}_q[X_1, \ldots, X_n]$ vanishing at S is $I = \langle g_1(X_1), \ldots, g_n(X_n) \rangle$, where $g_i(X_i) = \prod_{\alpha \in S_i} (X_i - \alpha)$ and $\deg(g_i) = m_i$ [8].

Consider the quotient ring $Q = \mathbb{F}_q[X_1, \ldots, X_n] / I$ and let

$$U = \{0, 1, \ldots, m_1 - 1\} \times \cdots \times \{0, 1, \ldots, m_n - 1\}.$$

An element $g \in Q$ is an equivalence class but we denote by g the unique polynomial in $\mathbb{F}_q[X_1, \ldots, X_n]$ with a degree in X_i less than m_i, $1 \leq i \leq n$, representing the equivalence class g, that is,

$$g(X_1, \ldots, X_n) = \sum_{(u_1, \ldots, u_n) \in U} g_{u_1, \ldots, u_n} X_1^{u_1} \cdots X_n^{u_n},$$

with $g_{u_1, \ldots, u_n} \in \mathbb{F}_q$. For each element $\mathbf{u} = (u_1, \ldots, u_n) \in U$, denote $X^{\mathbf{u}} = X_1^{u_1} \cdots X_n^{u_n}$. Set $\operatorname{supp}(g) = \{(u_1, \ldots, u_n) \in U \mid g_{u_1, \ldots, u_n} \neq 0\}$ and for every $\Delta \subseteq U$, define $G_\Delta := \{g \in Q \mid \operatorname{supp}(g) \subseteq \Delta\}$. Then, $G_\Delta = \langle X^{\mathbf{u}} \mid \mathbf{u} \in \Delta \rangle$. Consider the linear evaluation map

$$\operatorname{ev}^S \colon Q \to \mathbb{F}_q^m, \quad \operatorname{ev}^S(g) = (g(\boldsymbol{\gamma}_1), \ldots, g(\boldsymbol{\gamma}_m)).$$

Our supporting codes are the following evaluation codes:

$$C(S, \Delta) := \operatorname{ev}^S(G_\Delta) = \langle \operatorname{ev}^S(X^{\mathbf{u}}) \mid \mathbf{u} \in \Delta \rangle \subseteq \mathbb{F}_q^m.$$

Denoting R_t the set of t-roots of unity for some $t \mid q - 1$, a J-affine variety code is a code $C(S, \Delta)$ where each S_i is of the form R_t or $R_t \cup \{0\}$.

The length and dimension of a code $C(S, \Delta)$ are $m = \prod_{i=1}^n m_i$ and $k = \#\Delta$. The minimum distance d admits the following bound [4]:

$$d \geq d^* := d^*(C(S, \Delta)) := \min \left\{ \prod_{i=1}^n (m_i - u_i) \mid \mathbf{u} = (u_1, \ldots, u_n) \in \Delta \right\}.$$

A code $C(S, \Delta)$ is d^*-*optimal* if it is optimal and $d = d^*$.

Let us see how to use the codes $C(S, \Delta)$ for locally recoverable purposes.

Proposition 2.1. *For each $1 \leq i \leq n$, define the support of G_Δ at X_i as*

$$\operatorname{Supp}_{X_i}(G_\Delta) := \{u_i \in \{0, 1, \ldots, m_i - 1\} \mid \textit{there exists a monomial } X_1^{u_1} \cdots X_i^{u_i} \cdots X_n^{u_n} \textit{ in } G_\Delta\}.$$

Denote $k_i := \max(\operatorname{Supp}_{X_i}(G_\Delta))$ and $\mathcal{K}_i := \#\operatorname{Supp}_{X_i}(G_\Delta)$, where $\#$ means cardinality. Then, for each $1 \leq i \leq n$ such that $\mathcal{K}_i < m_i$, $C(S, \Delta)$ is a $(\geq \mathcal{K}_i, \leq m_i - \mathcal{K}_i + 1)$-locally recoverable code. If $\operatorname{Supp}_{X_i}(G_\Delta) = \{0, 1, \ldots, k_i\}$, then the locality is $(\mathcal{K}_i, m_i - \mathcal{K}_i + 1)$.

Sketch of the proof. Let $i \in \{1, \dots, n\}$. The position $c_j = g(\boldsymbol{\gamma}_j)$ of a codeword $\mathbf{c} = \mathrm{ev}^S(g) \in C(S, \Delta)$ can be recovered after certain interpolation with respect to X_i. Indeed, take the polynomial

$$g(X_1, \dots, X_n) = \sum_{h=0}^{k_i} f_h(X_1, \dots, X_{i-1}, X_{i+1}, \dots, X_n) X_i^h$$

in $\mathbb{F}_q[X_1, \dots, X_{i-1}, X_{i+1}, \dots, X_n][X_i]$. Considering the following subset of S:

$$\overline{R}_S := \left\{ (\gamma_{j_1}, \dots, \gamma_{j_{i-1}}, x, \gamma_{j_{i+1}}, \dots, \gamma_{j_n}) \mid x \in S_i \right\},$$

and replacing each X_l, $l \neq i$, in g by γ_{jl}, we obtain a polynomial in X_i with constant coefficients of degree at most k_i. So we can interpolate it by using $k_i + 1$ points in $\overline{R}_S$. However, since $f_h(X_1, \dots, X_{i-1}, X_{i+1}, \dots, X_n) = 0$ for all $h \notin \mathrm{Supp}_{X_i}(G_\Delta)$, we actually only need $\mathcal{K}_i$ points in $\overline{R}_S$ to obtain the coefficients of the polynomial in $\mathbb{F}_q[X_i]$. By taking

$$\overline{R} := \{t \in \{1, \dots, m\} \mid \boldsymbol{\gamma}_t \in \overline{R}_S\},$$

$r := m_i - \mathrm{d}(C[\overline{R}] + 1$ and $\delta := \mathrm{d}(C[\overline{R}])$, the result follows because $j \in \overline{R}$, $\#\overline{R} = m_i$ and $\mathrm{d}(C[\overline{R}]) \leq m_i - \mathcal{K}_i + 1$. When $\mathrm{Supp}_{X_i}(G_\Delta) = \{0, 1, \dots, k_i\}$, the claim follows straightforwardly since $C[\overline{R}]$ is a Reed-Solomon code (and thus an MDS code). □

3. Optimal (r, δ)-locally recoverable codes

In this last section we state the results mentioned in the introduction which determine several families of (r, δ)-locally recoverable codes of the type $C(S, \Delta)$.

Theorem 3.1. *Let $n = 2$ and $(i, j) \in \{(1, 2), (2, 1)\}$. The code $C(S, \Delta)$ is a d^*-optimal (r, δ)-locally recoverable code over $\mathbb{F}_q$ if and only if Δ is some of the following sets:*

(1) $\Delta^1_{v_i, v_j} := \{(u_1, u_2) \mid 0 \leq u_i \leq v_i,\ 0 \leq u_j \leq v_j\}$, *where the pair (v_i, v_j) satisfies one of the following conditions:*
   - $v_i = 0$ *and* $0 \leq v_j \leq m_j - 1$;
   - $1 \leq v_i \leq m_i - 2$ *and* $v_j = m_j - 1$;

(2) $\Delta^2_{v_i, s} := \{(u_1, u_2) \mid 0 \leq u_i \leq v_i,\ 0 \leq u_j \leq m_j - 2\} \cup \{(u_1, u_2) \mid 0 \leq u_i \leq s,\ u_j = m_j - 1\}$, *where* $\max\{0, 2v_i - m_i\} \leq s < v_i \leq m_i - 2$;

(3) $\Delta^3_{v_i, v_j} := \{(u_1, u_2) \mid 0 \leq u_i \leq v_i,\ 0 \leq u_j \leq v_j - 1\} \cup \{(u_1, u_2) \mid u_i = 0,\ u_j = v_j\}$, *where* $1 \leq v_i \leq m_i - 2$ *and* $\max\left\{1, \frac{v_i(m_j+1) - m_i}{v_i}\right\} \leq v_j \leq m_j - 2$.

In all cases, the locality is $(r, \delta) = (v_i + 1, m_i - v_i)$.

Theorem 3.2. *Let $n \geq 3$. For each index $i_0 \in \{1, \dots, n\}$, set $v_i = m_i - 1$ for all $i \in \{1, \dots, n\} \backslash \{i_0\}$ and take $v_{i_0} \in \{0, 1, \dots, m_{i_0} - 2\}$. Define*

$$\Delta^{1, i_0}_{v_1, \dots, v_m} = \{(u_1, \dots, u_n) \mid 0 \leq u_i \leq v_i, \text{ for all } i = 1, \dots, n\}.$$

Then the code $C(S, \Delta)$ is a d^*-optimal (r, δ)-locally recoverable code over $\mathbb{F}_q$ if and only if there is an index i_0 as above such that Δ is one of the following forms:

(1) $\Delta^{1, i_0}_{v_1, \dots, v_m}$; *or*

(2) $\Delta^{2, i_0}_{v_{i_0}, s} = \Delta^{1, i_0}_{v_1, \dots, v_m} \backslash \{(m_1 - 1, \dots, m_{i_0 - 1} - 1, u_{i_0}, m_{i_0 + 1} - 1, \dots, m_n - 1) \mid s \leq u_{i_0} \leq v_{i_0}\}$, *where s satisfies* $\max\{1, 2v_{i_0} - m_{i_0}\} \leq s \leq v_{i_0} \leq m_{i_0} - 2$ *or* $v_{i_0} = s = 0$.

In both cases, the locality is $(r, \delta) = (v_{i_0} + 1, m_{i_0} - v_{i_0})$.

Set $q = 11$, $m_1 = 10$, $m_2 = 9$ and $(i, j) = (1, 2)$. Figure 1 represents U where each element (u_1, u_2) is labelled with the integer $(m_1 - u_1)(m_2 - u_2)$. The shaded area on the left (resp., right) represents $\Delta^3_{2,7}$ (resp., $\Delta^2_{7,4}$) in Theorem 3.1. The parameters and locality (r, δ) of $C(S, \Delta^3_{2,7})$ (resp., $\Delta^2_{7,4}$) are $[90, 22, 20]$ and $(3, 8)$ (resp., $[90, 69, 6]$ and $(8, 3)$).

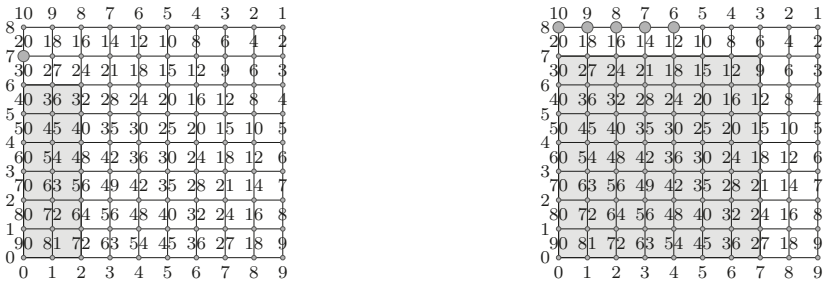


FIGURE 1. Sets $\Delta^3_{2,7}$ and $\Delta^2_{7,4}$ of Theorem 3.1 for $q = 11$, $m_1 = 10$, $m_2 = 9$

REFERENCES

[1] B. CHEN, W. FANG, S.-T. XIA AND F.-W. FU, Constructions of optimal (r, δ) locally repairable codes via constacyclic codes, *IEEE Trans. Commun. 67(8)* (2019) 5253-5263.
[2] B. CHEN, S-T. XIA, J. HAO AND F-W. FU, Constructions of optimal cyclic (r, δ) locally repairable codes, *IEEE Trans. Inform. Theory 64(4)* (2018) 2499-2511.
[3] W. FANG AND F.W. FU, Optimal cyclic (r, δ) locally repairable codes with unbounded length, *Finite Fields Appl. 63* (2020) 101650, 14 pp.
[4] O. GEIL, S. MARTIN, R. MATSUMOTO, D. RUANO AND Y. LUO, Relative generalized Hamming weights of one-point algebraic geometric codes, *IEEE Trans. Inform. Theory 60(10)* (2014) 5938-5949.
[5] P. GOPALAN, C. HUANG, H. SIMITCI AND S. YEKHANIN, On the locality of codeword symbols, *IEEE Trans. Inform. Theory 58(11)* (2012) 6925-6934.
[6] J. LIU, S. MESNAGER AND L. CHEN, New constructions of optimal locally recoverable codes via good polynomials, *IEEE Trans. Inform. Theory 64(2)* (2018) 889-899.
[7] J. LIU, S. MESNAGER AND D. TANG, Constructions of optimal locally recoverable codes via Dickson polynomials, *Des. Codes Cryptogr. 88* (2020) 1759-1780.
[8] H. H. LÓPEZ, C. RENTERÍA-MÁRQUEZ AND R. H. VILLARREAL, Affine cartesian codes, *Des. Codes Cryptogr. 71* (2014) 5-19.
[9] N. PRAKASH, G. M. KAMATH, V. LALITHA AND P. V. KUMAR, Optimal linear codes with a local-error-correction property, in *Proceedings of IEEE Int. Symp. Inform. Theory (ISIT-2012)* (2012) 2776-2780.
[10] J. QIU, D. ZHENG AND F. -W. FU, New constructions of optimal cyclic (r, δ) locally repairable codes from their zeros, *IEEE Trans. Inform. Theory 67(3)* (2021) 1596-1608.
[11] C. SALGADO, A. VARILLY-ALVARADO AND J.F. VOLOCH, Locally recoverable codes on surfaces, *IEEE Trans. Inform. Theory 67(9)* (2021) 5765-5777.
[12] Z. ZHANG, J. XU AND M. LIU, Constructions of optimal locally repairable codes over small fields, *Sci. Sin. Math. 47(11)* (2017) 1607-1614.

Universitat Jaume I
Email address: martinh@uji.es

DOUBLY EXTENDED CODES FOR GENERAL METRICS

UMBERTO MARTÍNEZ-PEÑAS

Abstract. In this work, doubly extended codes are generalized to any metric and to any initial code to be extended. In particular, doubly extended maximum sum-rank distance (MSRD) codes are obtained from several families of known MSRD codes. These results generalize classical doubly extended Reed–Solomon codes for the Hamming metric and the recent doubly extended linearized Reed–Solomon codes for the sum-rank metric.

1. Introduction

Doubly extended Reed–Solomon codes are the linear codes in $\mathbb{F}_q^{n+2}$ with generator matrix

$$\left(\begin{array}{cccc|cc} 1 & 1 & \dots & 1 & 1 & 0 \\ a_1 & a_2 & \dots & a_n & 0 & 0 \\ a_1^2 & a_2^2 & \dots & a_n^2 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ a_1^{k-2} & a_2^{k-2} & \dots & a_n^{k-2} & 0 & 0 \\ a_1^{k-1} & a_2^{k-1} & \dots & a_n^{k-1} & 0 & 1 \end{array}\right) \in \mathbb{F}_q^{k\times(n+2)},$$

for distinct $a_1, a_2, \dots, a_n \in \mathbb{F}_q^*$ (hence $n \leq q-1$ and $n+2 \leq q+1$, where equalities may be attained). These codes are maximum distance separable (MDS), i.e., their minimum Hamming distance attains the Singleton bound. Furthermore, these codes have a length of $q+1$, which is conjectured to be maximum for most values of the code dimension (*MDS conjecture*). In fact, this is true for q prime [1].

A generalization of this result to the sum-rank metric was recently given in [4]. The generalization of Reed–Solomon codes to the sum-rank metric is called linearized Reed–Solomon codes, introduced in [3]. The authors of [4] introduced doubly extended linearized Reed–Solomon codes and used geometric tools to show that these codes are maximum sum-rank distance (MSRD) codes, i.e., they attain the Singleton bound for the sum-rank metric.

In this work, we show that we may doubly extend codes attaining the Singleton bound for any metric given by a weight, extending the results above for the Hamming and sum-rank metrics. We provide necessary and sufficient conditions for the doubly extended code to attain the Singleton bound based on the original code. We conclude by doubly extending the general family of MSRD codes from [2], generalizing the result in [4].

2. General doubly extended codes

In this work, we consider metrics given by a weight, i.e., $\mathrm{d}(\mathbf{c},\mathbf{d}) = \mathrm{wt}(\mathbf{c}-\mathbf{d})$, where

The author has been partially supported by a María Zambrano contract from the Universidad de Valladolid.

The talk at the EACA 2022 meeting was given by the first named author.

(1) $\mathrm{wt}(\mathbf{c}) \geq 0$ and it equals 0 if, and only if, $\mathbf{c} = \mathbf{0}$, for all $\mathbf{c} \in \mathbb{F}_q^n$,
(2) $\mathrm{wt}(\lambda\mathbf{c}) = \mathrm{wt}(\mathbf{c})$, for all $\mathbf{c} \in \mathbb{F}_q^n$ and all $\lambda \in \mathbb{F}_q^*$,
(3) $\mathrm{wt}(\mathbf{c}+\mathbf{d}) \leq \mathrm{wt}(\mathbf{c}) + \mathrm{wt}(\mathbf{d})$, for all $\mathbf{c}, \mathbf{d} \in \mathbb{F}_q^n$,

for $\mathbf{c}, \mathbf{d} \in \mathbb{F}_q^n$. Furthermore, we also restrict our study to metrics given by weights that satisfy the Singleton bound: $\mathrm{d}(\mathcal{C}) \leq n - k + 1$, where $k = \log_q |\mathcal{C}|$, for any code $\mathcal{C} \subseteq \mathbb{F}_q^n$, where $\mathrm{d}(\mathcal{C}) = \min\{\mathrm{d}(\mathbf{c}, \mathbf{d}) \mid \mathbf{c}, \mathbf{d} \in \mathcal{C}, \mathbf{c} \neq \mathbf{d}\}$. We define the Hamming weight of $\mathbf{c} \in \mathbb{F}_q^n$ as $\mathrm{wt}_H(\mathbf{c}) = |\{i \in [n] \mid c_i \neq 0\}|$ and we denote the corresponding metric by d_H.

The following theorem is our main result.

Theorem 2.1. *Let $\mathcal{C} \subseteq \mathbb{F}_q^n$ be a k-dimensional linear code generated by $\mathbf{g}_1, \mathbf{g}_2, \ldots, \mathbf{g}_k \in \mathbb{F}_q^n$. Define the codes $\mathcal{C}_k = \langle \mathbf{g}_1, \ldots, \mathbf{g}_{k-1} \rangle$, $\mathcal{C}_1 = \langle \mathbf{g}_2, \ldots, \mathbf{g}_k \rangle$ and $\mathcal{C}_{1,k} = \langle \mathbf{g}_2, \ldots, \mathbf{g}_{k-1} \rangle$. Then the k-dimensional linear code $\mathcal{C}_e \subseteq \mathbb{F}_q^{n+2}$ with generator matrix*

$$G_e = \left(\begin{array}{c|cc} \mathbf{g}_1 & 1 & 0 \\ \hline \mathbf{g}_2 & 0 & 0 \\ \vdots & \vdots & \vdots \\ \mathbf{g}_{k-1} & 0 & 0 \\ \hline \mathbf{g}_k & 0 & 1 \end{array}\right) \in \mathbb{F}_q^{k \times (n+2)}$$

satisfies $\mathrm{d}_e(\mathcal{C}_e) = \min\{\mathrm{d}(\mathcal{C}) + 2, \mathrm{d}(\mathcal{C}_1) + 1, \mathrm{d}(\mathcal{C}_k) + 1, \mathrm{d}(\mathcal{C}_{1,k})\}$, where the metrics are given by

$$\mathrm{d}_e((\mathbf{c}, c_{n+1}, c_{n+2}), (\mathbf{d}, d_{n+1}, d_{n+2})) = \mathrm{d}(\mathbf{c}, \mathbf{d}) + \mathrm{d}_H((c_{n+1}, c_{n+2}), (d_{n+1}, d_{n+2})),$$

for $\mathbf{c}, \mathbf{d} \in \mathbb{F}_q^n$ and $c_{n+1}, c_{n+2}, d_{n+1}, d_{n+2} \in \mathbb{F}_q$.

Proof. Note that a codeword in $\mathcal{C}_e$ is of the form

$$\mathbf{c} = \left(\sum_{i=1}^{k} \lambda_i \mathbf{g}_i, \lambda_1, \lambda_k \right),$$

where $\lambda_1, \lambda_2, \ldots, \lambda_k \in \mathbb{F}_q$. Hence

$$\mathrm{wt}_e(\mathbf{c}) = \mathrm{wt}\left(\sum_{i=1}^{k} \lambda_i \mathbf{g}_i \right) + \mathrm{wt}_H\left(\lambda_1, \lambda_k\right).$$

We therefore easily deduce that $\mathrm{d}_e(\mathcal{C}_e) \geq \min\{\mathrm{d}(\mathcal{C}) + 2, \mathrm{d}(\mathcal{C}_1) + 1, \mathrm{d}(\mathcal{C}_k) + 1, \mathrm{d}(\mathcal{C}_{1,k})\}$.

To see that equality can be attained, we need to consider the four cases (1) $\lambda_1 = \lambda_k = 0$, (2) $\lambda_1 = 0$ and $\lambda_k \neq 0$, (3) $\lambda_1 \neq 0$ and $\lambda_k = 0$, and (4) $\lambda_1 \neq 0 \neq \lambda_k$. In the first case, if we take $\mathbf{c} \in \mathcal{C}_{1,k}$ with $\mathrm{wt}(\mathbf{c}) = \mathrm{d}(\mathcal{C}_{1,k})$, then $\mathrm{wt}_e(\mathbf{c}, 0, 0) = \mathrm{wt}(\mathbf{c})$. We now turn to the second case. Let $\mathbf{c} \in \mathcal{C}_{1,k}$ and $\lambda_k \in \mathbb{F}_q$ such that $\mathrm{wt}(\mathbf{c} + \lambda_k \mathbf{g}_k) = \mathrm{d}(\mathcal{C}_1)$. If $\lambda_k = 0$, then we are in the first case and $\mathrm{d}(\mathcal{C}_{1,k}) = \mathrm{wt}(\mathbf{c}) = \mathrm{d}(\mathcal{C}_1)$. If $\lambda_k \neq 0$, then we are subject to the second case and $\mathrm{wt}_e(\mathbf{c} + \lambda_k \mathbf{g}_k, 0, \lambda_k) = \mathrm{d}(\mathcal{C}_1) + 1$. We can treat the other two cases similarly, and we finally see that the equality $\mathrm{d}_e(\mathcal{C}_e) = \min\{\mathrm{d}(\mathcal{C}) + 2, \mathrm{d}(\mathcal{C}_1) + 1, \mathrm{d}(\mathcal{C}_k) + 1, \mathrm{d}(\mathcal{C}_{1,k})\}$ is attained. □

The following consequence is straightforward by looking at the code dimensions.

Corollary 2.2. *With notation as in Theorem 2.1, the code $\mathcal{C}_e$ attains the Singleton bound for d_e if, and only if, so do the four codes $\mathcal{C}$, $\mathcal{C}_1$, $\mathcal{C}_k$ and $\mathcal{C}_{1,k}$ for d.*

3. Doubly extended MSRD codes

In this section, we generalize the construction of doubly extended linearized Reed–Solomon codes from [4] to the general family of MSRD codes from [2]. Recall that the sum-rank metric in $\mathbb{F}_{q^m}^n$ over $\mathbb{F}_q$ for the length partition (g,r) is defined as a sum of rank metrics, i.e., sum-rank weights are given by $\mathrm{wt}_{SR}(\mathbf{c}) = \sum_{i=1}^{g} \mathrm{wt}_R\left(\mathbf{c}^{(i)}\right)$, for $\mathbf{c} = \left(\mathbf{c}^{(1)}, \mathbf{c}^{(2)}, \ldots, \mathbf{c}^{(g)}\right) \in \mathbb{F}_{q^m}^n$, where $\mathbf{c}^{(i)} \in \mathbb{F}_{q^m}^r$, for $i = 1, 2, \ldots, g$, and $n = gr$. Recall that rank weights in $\mathbb{F}_{q^m}^r$ are given by $\mathrm{wt}_R(\mathbf{d}) = \dim_{\mathbb{F}_q}(\langle d_1, d_2, \ldots, d_r\rangle_{\mathbb{F}_q})$, for $\mathbf{d} = (d_1, d_2, \ldots, d_r) \in \mathbb{F}_{q^m}^r$.

We now give the definition of extended Moore matrices from [2].

Definition 3.1 ([2])**.** Let $\mathbf{a} = (a_1, a_2, \ldots, a_\ell) \in (\mathbb{F}_{q^m}^*)^\ell$ be such that $N_{\mathbb{F}_{q^m}/\mathbb{F}_q}(a_i) \neq N_{\mathbb{F}_{q^m}/\mathbb{F}_q}(a_j)$ if $i \neq j$, where $N_{\mathbb{F}_{q^m}/\mathbb{F}_q}$ denotes the norm of the extension $\mathbb{F}_q \subseteq \mathbb{F}_{q^m}$. Let $\boldsymbol{\beta} = (\beta_1, \beta_2, \ldots, \beta_{\mu r}) \in \mathbb{F}_{q^m}^{\mu r}$ be an arbitrary vector for the positive integers μ and r. For $k = 1, 2, \ldots, n = \ell\mu r$, we define the *extended Moore matrix* $M_k(\mathbf{a}, \boldsymbol{\beta}) \in \mathbb{F}_{q^m}^{k\times n}$ by $M_k(\mathbf{a}, \boldsymbol{\beta}) =$

$$\left(\begin{array}{ccc|c|ccc} \beta_1 & \cdots & \beta_{\mu r} & \cdots & \beta_1 & \cdots & \beta_{\mu r} \\ \beta_1^q a_1 & \cdots & \beta_{\mu r}^q a_1 & \cdots & \beta_1^q a_\ell & \cdots & \beta_{\mu r}^q a_\ell \\ \beta_1^{q^2} a_1^{\frac{q^2-1}{q-1}} & \cdots & \beta_{\mu r}^{q^2} a_1^{\frac{q^2-1}{q-1}} & \cdots & \beta_1^{q^2} a_\ell^{\frac{q^2-1}{q-1}} & \cdots & \beta_{\mu r}^{q^2} a_\ell^{\frac{q^2-1}{q-1}} \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ \beta_1^{q^{k-1}} a_1^{\frac{q^{k-1}-1}{q-1}} & \cdots & \beta_{\mu r}^{q^{k-1}} a_1^{\frac{q^{k-1}-1}{q-1}} & \cdots & \beta_1^{q^{k-1}} a_\ell^{\frac{q^{k-1}-1}{q-1}} & \cdots & \beta_{\mu r}^{q^{k-1}} a_\ell^{\frac{q^{k-1}-1}{q-1}} \end{array}\right),$$

and we denote by $\mathcal{C}_k(\mathbf{a}, \boldsymbol{\beta}) \subseteq \mathbb{F}_{q^m}^n$ the k-dimensional linear code generated by $M_k(\mathbf{a}, \boldsymbol{\beta})$.

Sufficient and necessary conditions for extended Moore matrices to yield MSRD codes over $\mathbb{F}_q$ for the length partition (g,r), $g = \ell\mu$, are given in [2] based on properties of the evaluation points $\beta_1, \beta_2, \ldots, \beta_{\mu r}$. Several constructions of MSRD codes based on such conditions were obtained in [2], including linearized Reed–Solomon codes [3].

For our purposes, we also need to consider the k-dimensional linear codes $\mathcal{D}_k(\mathbf{a}, \boldsymbol{\beta}) \subseteq \mathbb{F}_{q^m}^n$ with generator matrix $M'_k(\mathbf{a}, \boldsymbol{\beta}) =$

$$\left(\begin{array}{ccc|c|ccc} \beta_1^q a_1 & \cdots & \beta_{\mu r}^q a_1 & \cdots & \beta_1^q a_\ell & \cdots & \beta_{\mu r}^q a_\ell \\ \beta_1^{q^2} a_1^{\frac{q^2-1}{q-1}} & \cdots & \beta_{\mu r}^{q^2} a_1^{\frac{q^2-1}{q-1}} & \cdots & \beta_1^{q^2} a_\ell^{\frac{q^2-1}{q-1}} & \cdots & \beta_{\mu r}^{q^2} a_\ell^{\frac{q^2-1}{q-1}} \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ \beta_1^{q^k} a_1^{\frac{q^k-1}{q-1}} & \cdots & \beta_{\mu r}^{q^k} a_1^{\frac{q^k-1}{q-1}} & \cdots & \beta_1^{q^k} a_\ell^{\frac{q^k-1}{q-1}} & \cdots & \beta_{\mu r}^{q^k} a_\ell^{\frac{q^k-1}{q-1}} \end{array}\right),$$

for $k = 1, 2, \ldots, n$. Note that in order to apply Corollary 2.2, we need the codes $\mathcal{D}_k(\mathbf{a}, \boldsymbol{\beta})$ to be MSRD. We now show that this is equivalent to $\mathcal{C}_k(\mathbf{a}, \boldsymbol{\beta})$ being MSRD.

Lemma 3.2. *Let $\mathbf{a} = (a_1, a_2, \ldots, a_\ell) \in (\mathbb{F}_{q^m}^*)^\ell$ be as in Definition 3.1. For $k = 1, 2, \ldots, n-1$, $\mathcal{C}_k(\mathbf{a}, \boldsymbol{\beta})$ is MSRD if, and only if, so is $\mathcal{D}_k(\mathbf{a}, \boldsymbol{\beta})$, over $\mathbb{F}_q$ for the length partition (g,r). Furthermore, the conditions for this to happen are independent of $1 \leq k \leq n-1$ (see* [2]*).*

Proof. For $a, \beta \in \mathbb{F}_{q^m}$ and a positive integer i, we have

$$\beta^{q^i} a^{\frac{q^i-1}{q-1}} = \beta^{q^i} a^{q^{i-1}} \cdots a^q \cdot a = \left(\beta^{q^{i-1}} a^{q^{i-2}} \cdots a^q \cdot a\right)^q a = \left(\beta^{q^{i-1}} a^{\frac{q^{i-2}-1}{q-1}}\right)^q a.$$

Hence it holds that $M'_k(\mathbf{a},\boldsymbol{\beta}) = M_k(\mathbf{a},\boldsymbol{\beta})^q \mathrm{diag}(a_1,\dots,a_1|\dots|a_\ell,\dots,a_\ell)$, where $M_k(\mathbf{a},\boldsymbol{\beta})^q$ means that we raise every entry of $M_k(\mathbf{a},\boldsymbol{\beta})$ to the qth power. In particular, the same holds for the corresponding codes, i.e., $\mathcal{D}_k(\mathbf{a},\boldsymbol{\beta}) = \mathcal{C}_k(\mathbf{a},\boldsymbol{\beta})^q \mathrm{diag}(a_1,\dots,a_1|\dots|a_\ell,\dots,a_\ell)$, where $\mathcal{C}_k(\mathbf{a},\boldsymbol{\beta})^q$ means that we raise every component of every codeword of $\mathcal{C}_k(\mathbf{a},\boldsymbol{\beta})$ to the qth power. Now observe that the map $\phi : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_{q^m}^n$ given by

$$\phi\left(c_1,\dots,c_{\mu r}|\dots|c_{(\ell-1)(\mu r)+1},\dots,c_{\ell(\mu r)}\right) = \left(c_1^q a_1,\dots,c_{\mu r}^q a_1|\dots|c_{(\ell-1)(\mu r)+1}^q a_\ell,\dots,c_{\ell(\mu r)}^q a_\ell\right)$$

is a semilinear isometry for the sum-rank metric over $\mathbb{F}_q$ for the length partition (g,r), since $a_i \neq 0$, for $i = 1,2,\dots,\ell$. Hence the result follows. □

We are therefore in the situation of Corollary 2.2 for the sum-rank metric. For this reason, we define the following codes.

Definition 3.3. Let $\mathbf{a} = (a_1,a_2,\dots,a_\ell) \in (\mathbb{F}_{q^m}^*)^\ell$ be as in Definition 3.1. Let $\boldsymbol{\beta} = (\beta_1,\beta_2,\dots,\beta_{\mu r}) \in \mathbb{F}_{q^m}^{\mu r}$ be an arbitrary vector. For $k = 2,3,\dots,n$, we define the *doubly extended Moore matrix* $M_k^e(\mathbf{a},\boldsymbol{\beta}) \in \mathbb{F}_{q^m}^{k\times(n+2)}$ by $M_k^e(\mathbf{a},\boldsymbol{\beta}) =$

$$\left(\begin{array}{ccc|c|ccc|cc}
\beta_1 & \dots & \beta_{\mu r} & \dots & \beta_1 & \dots & \beta_{\mu r} & 1 & 0 \\
\beta_1^q a_1 & \dots & \beta_{\mu r}^q a_1 & \dots & \beta_1^q a_\ell & \dots & \beta_{\mu r}^q a_\ell & 0 & 0 \\
\beta_1^{q^2} a_1^{\frac{q^2-1}{q-1}} & \dots & \beta_{\mu r}^{q^2} a_1^{\frac{q^2-1}{q-1}} & \dots & \beta_1^{q^2} a_\ell^{\frac{q^2-1}{q-1}} & \dots & \beta_{\mu r}^{q^2} a_\ell^{\frac{q^2-1}{q-1}} & 0 & 0 \\
\vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots & \vdots & \vdots \\
\beta_1^{q^{k-1}} a_1^{\frac{q^{k-1}-1}{q-1}} & \dots & \beta_{\mu r}^{q^{k-1}} a_1^{\frac{q^{k-1}-1}{q-1}} & \dots & \beta_1^{q^{k-1}} a_\ell^{\frac{q^{k-1}-1}{q-1}} & \dots & \beta_{\mu r}^{q^{k-1}} a_\ell^{\frac{q^{k-1}-1}{q-1}} & 0 & 1
\end{array}\right),$$

and we denote by $\mathcal{C}_k^e(\mathbf{a},\boldsymbol{\beta}) \subseteq \mathbb{F}_{q^m}^{n+2}$ the k-dimensional linear code generated by $M_k^e(\mathbf{a},\boldsymbol{\beta})$.

Thus by Corollary 2.2 and Lemma 3.2, we deduce the following.

Theorem 3.4. *Let $\mathbf{a} = (a_1,a_2,\dots,a_\ell) \in (\mathbb{F}_{q^m}^*)^\ell$ be as in Definition 3.1. For $k = 2,3,\dots,n$, $\mathcal{C}_k(\mathbf{a},\boldsymbol{\beta}) \subseteq \mathbb{F}_{q^m}^n$ is MSRD if, and only if, so is $\mathcal{C}_k^e(\mathbf{a},\boldsymbol{\beta}) \subseteq \mathbb{F}_{q^m}^{n+2}$ for the metric*

$$\mathrm{d}_e((\mathbf{c},c_{n+1},c_{n+2}),(\mathbf{d},d_{n+1},d_{n+2})) = \mathrm{d}_{SR}(\mathbf{c},\mathbf{d}) + \mathrm{d}_H((c_{n+1},c_{n+2}),(d_{n+1},d_{n+2})),$$

for $\mathbf{c},\mathbf{d} \in \mathbb{F}_{q^m}^n$ and $c_{n+1},c_{n+2},d_{n+1},d_{n+2} \in \mathbb{F}_{q^m}$, where d_{SR} denotes the sum-rank metric in $\mathbb{F}_{q^m}^n$ over $\mathbb{F}_q$ for the length partition (g,r).

Thus all of the MSRD codes from [2] may be doubly extended as above.

References

[1] S. Ball. On sets of vectors of a finite vector space in which every subset of basis size is a basis. *Journal of the European Mathematical Society*, 14(3):733–748, 2012.

[2] U. Martínez-Peñas. A general family of MSRD codes and PMDS codes with smaller field sizes from extended Moore matrices. Preprint: arXiv:2011.14109.

[3] U. Martínez-Peñas. Skew and linearized Reed–Solomon codes and maximum sum rank distance codes over any division ring. *J. Algebra*, 504:587–612, 2018.

[4] A. Neri, P. Santonastaso, and F. Zullo. The geometry of one-weight codes in the sum-rank metric. 2021. Preprint: arXiv:2112.04989.

IMUVa-Mathematics Research Institute, University of Valladolid, Spain
Email address: umberto.martinez@uva.es

A GENERALIZATION OF EFFECTIVE SERRE SPECTRAL SYSTEMS FOR m-MULTICOMPLEXES

DANIEL MIGUEL, ANDREA GUIDOLIN, ANA ROMERO, AND JULIO RUBIO

Abstract. In a previous study [2], we gave an algorithm to construct a spectral system from a tower of fibrations of simplicial sets, which encompasses all the information provided by the successive Serre spectral sequences of each fibration. The spectral system was built over generalized multicomplexes that come from the associated chain complexes of the simplicial sets. In this work we show that a similar spectral system can be constructed over a broader class of multicomplexes, and that we have effective homology for it.

Introduction

A spectral system is an algebraic construction that was introduced by Benjamin Matschke in [4]. It generalizes classical spectral sequences, allowing the treatment of more complex structures and combinations of them. However, these richer structures also present similar computational problems, such as the non-existence of algorithms to compute differentials and the finiteness of the involved mathematical objects. These problems can be solved for concrete situations using the effective homology technique [8], as was shown in a series of works including [3] and [6]. As a consequence, despite the existence of a broader theoretical setting, we are restricted to the framework of previous computational works, based on generalized filtered chain complexes of free $\mathbb{Z}$-modules.

A generalized filtered chain complex is a chain complex (C_*, d) together with a family of subcomplexes $\{F_iC_*\}_{i\in I}$ indexed by a poset I such that $F_iC_n \subseteq F_jC_n$ if $i \leq j$ and $n \in \mathbb{Z}$. A spectral system [4] over C_* is defined by taking the quotients

$$S_n\,[z,s,p,b] = \frac{F_pC_n \cap d^{-1}(F_zC_{n-1})}{d(F_bC_{n+1}) + F_sC_n},$$

for $z \leq s \leq p \leq b \in I$, together with the induced differentials. We will work with the poset $D(\mathbb{Z}^m)$ of downsets of $\mathbb{Z}^m$, which are subsets p of $\mathbb{Z}^m$ such that if $(p_1, ..., p_m) \in p$, then $(q_1, ..., q_m) \in p$ if $q_i \leq p_i$ for $i = 1, ..., m$.

Whenever a chain complex presents computational setbacks, we try to find an equivalent chain complex where we can work out our problem. On the one hand, a reduction $C_* \Rightarrow\!\!\!\!\!\rightarrow D_*$ between two chain complexes is a triple (f, g, h) ($f : C_* \to D_*$, $g : D_* \to C_*$ and $h : C_* \to C_{*+1}$) such that f and g are chain complex morphisms, $fg = \mathrm{Id}_D$, $gf + d_Ch + hd_C = \mathrm{Id}_C$, $fh = 0$, $hg = 0$ and $hh = 0$. And on the other hand, a chain complex is said to be effective if it is finitely generated (with distinguishable basis) and has computable differentials. Finally,

This work was supported by grants PID2020-115225RB-I00 and PID2020-116641GB-I00 funded by MCIN/ AEI/ 10.13039/501100011033, and by the Wallenberg AI, Autonomous Systems and Software Program (WASP) funded by the Knut and Alice Wallenberg Foundation.

The talk at the EACA 2022 meeting was given by the first named author.

we say that a chain complex has effective homology if there is a chain of reductions from itself to an effective chain complex. Effective homology was introduced by Francis Sergeraert (see [8], [7]), and it is implemented for several problems in the program Kenzo ([1]).

The usual setup for this kind of object comes from a more topological framework, by means of fibrations (twisted cartesian products) of simplicial sets and associated chain complexes. That is the case of the Serre homology spectral sequence for towers of fibrations, which was successfully tackled in [2]. This work will serve us as guide, as we explain in the next section. Another example is the more recent work [5], concerning both Eilenberg–Moore and Serre spectral sequences.

1. Systems of towers of fibrations

A tower of fibrations consists of m ordered fibrations such that the total space of each fibration is the base of the next one. Knowing the homology of the first base space and the homology of all the fibers, it is possible to use the homology Serre spectral sequence successively, and determine the homology of the last total space (up to differential and extension problems). However, in [4] the author provided a new theoretical approach through spectral systems, and in our previous work [2] a constructive version was proved for twisted cartesian products of simplicial sets and implemented in Kenzo. The main results of [2] can be summed up in the following theorem.

Theorem 1.1. *Let $G_0, ..., G_{m-1}$ be simplicial groups, and let $E_0, ..., E_{m-1}, B$ be simplicial sets. Suppose that we have a tower of m fibrations, $G_i \to E_i \to E_{i+1}$ for $0 \leq i < m-1$ and $G_{m-1} \to E_{m-1} \to B$, given all of them by twisted cartesian products ($E_i \cong G_i \times_{\tau_i} E_{i+1}$, $E_{m-1} \cong G_{m-1} \times_{\tau_m} B$). If $G_0, ..., G_{m-1}, B$ are 1-reduced and have effective homology, then*

- *we can construct a spectral system over $D(\mathbb{Z}^m)$, by means of Serre filtrations, over the chain complex $C_*(G_0 \times_{\tau_0} (G_1 \times_{\tau_1} (...(G_{m-1} \times_{\tau_m} B)...)))$. The terms of the 2-page are given by:*

$$S_n(P; m) = H_{p_m}(B; H_{p_{m-1}}(G_{m-1}; ...H_{p_1}(G_1; H_{p_0}(G_0)),$$

  with $P := (p_1, ..., p_m) \in \mathbb{Z}^m$ and $p_0 := n - p_1 - ... - p_m$. Moreover, the spectral system converges to $H(E_0)$.
- *We have effective homology for the complex $C_*(G_0 \times_{\tau_0} (G_1 \times_{\tau_1} (...(G_{m-1} \times_{\tau_m} B)...)))$, and we can define a spectral system over the correspondent effective chain complex isomorphic to the previous one from the 2-page.*

To prove this result, on the one hand, we give effective homology for $C_*(G_0 \times_{\tau_0} (G_1 \times_{\tau_1} (...(G_{m-1} \times_{\tau_m} B)...)))$. First, successive applications of the Twisted Eilenberg-Zilber theorem (which involves the Basic Perturbation Lemma, see [7]) give us the perturbed chain complex $C_* := C_*(G_0) \otimes_{t_0} (C_*(G_1) \otimes_{t_1} (... \otimes_{t_{m-2}} (C_*(G_{m-1}) \otimes_{t_{m-1}} C_*(B))...))$. Its differential can be seen as $d_C = d_\otimes + \delta_C$, $d_\otimes$ being the differential of the usual tensor product and δ_C being the resulting perturbation from those successive applications of the mentioned theorem. Finally, we give effective homology for C_*, by taking the tensor products of the reductions for the factors of C_* and adding δ_C as a perturbation.

On the other hand, we define the filtrations that determine the Serre spectral sequence. These are defined using the downsets T^m_P, introduced in [4]. Consider the function $\phi : \mathbb{Z}^m \to \mathbb{Z}^m$, given by $\phi(x_1, ..., x_m) = (\sum_{i=1}^m x_i, \sum_{i=2}^m x_i, ..., x_m)$. We define T^m_P, for $P \in \mathbb{Z}^m$, to be

the set $\{X \in \mathbb{Z}^m | \phi(X) \leq_{lex} \phi(P)\}$, $\leq_{lex}$ being the lexicographic order. For these filtrations to be well defined, they must have good behaviour with respect to d_C and the other (similar) differentials of the complexes involved in the reductions. Moreover, one must prove that the nilpotency conditions which are necessary hypotheses for the Perturbation Lemma (see [7]) are satisfied. This is achieved as a consequence of the following:

1) We have a generalized filtration over $D(\mathbb{Z}^m)$ on C_* defined by means of the downsets of the form T^m_P, $P \in \mathbb{Z}^m$. We consider the modules of the form $C_{j_0}(G_0) \otimes_{t_0} (C_{j_1}(G_1) \otimes_{t_1} (... \otimes_{t_{m-2}} (C_{j_{m-1}}(G_{m-1}) \otimes_{t_{m-1}} C_{j_m}(B))...))$ on that complex and for each of its generators σ, we put $J_\sigma := (j_1, ..., j_m)$. Then $F_{T^m_P}$ is defined to be the free $\mathbb{Z}$-module generated by the $\sigma \in C_*$ such that $J_\sigma \in T^m_P$. Then it is extended naturally to the whole $\mathbb{Z}^m$.
2) The perturbation δ_C of the differential on C_* can be expressed as $\delta_C = \delta_0 + \mathrm{Id}_{G_0} \otimes \delta_1 + ... + \mathrm{Id}_{G_0 ... G_{m-2}} \otimes \delta_{m-1}$. Each of the δ_i decreases the degree of $C_*(G_{i+1}) \otimes_{t_{i+1}} ... \otimes_{t_{m-1}} C_*(B)$ by at least two units. This implies that the differential d_C is compatible with the filtration ($d(F_{T^m_P}) \subseteq F_{T^m_P}$) and that in addition, the nilpotency conditions for the perturbation lemmas are satisfied.

2. Generalization for multicomplexes

The goal of this work is to look for more general complexes that can take the place of C_*, suitable for the spectral system and the effective homology. We define the following objects:

Definition 2.1. An m-multicomplex M_* is a collection of modules over a ring indexed over $\mathbb{Z}^{m+1}$ with homomorphisms $d_{i_0,...,i_{m-1}} : M_{j_0,...,j_m} \to M_{j_0+i_0-1,...,j_{m-1}+i_{m-1}-i_{m-2},j_m-i_{m-1}}$ of multidegree $(i_0 - 1, i_1 - i_0, ..., i_{m-1} - i_{m-2}, -i_{m-1})$, with $i_0, ..., i_{m-1} \in \mathbb{Z}_{\geq 0}$, such that $\sum_{i_0+l_0=k_0,...,i_{m-1}+l_{m-1}=k_{m-1}} d_{i_0,...,i_{m-1}} d_{l_0,...,l_{m-1}} = 0$, for some $k_0, ..., k_{m-1}$ in $\mathbb{Z}$.

For $m = 1$, we recover the standard definition of multicomplex [9]. The complex C_* of the previous section can be seen as m-multicomplex, by first taking $M_{j_0,...,j_m} = C_{j_0}(G_0) \otimes_{t_0} (C_{j_1}(G_1) \otimes_{t_1} (... \otimes_{t_{m-2}} (C_{j_{m-1}}(G_{m-1}) \otimes_{t_{m-1}} C_{j_m}(B))...))$. Then we can see the untwisted tensor product's differential as different arrows with multidegrees $i_l = 0$ for $l \geq k$ and $i_l = 1$ for $l < k$, $k = 0, ..., m$. The other perturbations δ_k have indexes $i_l = 1$ for $l < k$ and $i_l \geq 2$ for $l \geq k$, $k = 0, ..., m - 1$. However, we have now more possibilities, since it does not have to come from a twisted cartesian product. Reciprocally, an m-multicomplex gives a chain complex by considering its totalization.

As with C_*, we can see every multicomplex as a perturbed version of a simpler multicomplex (corresponding to the untwisted tensor product). Indeed, we can take the arrows that correspond to the tensor product's differential, $d_\otimes$, described in the previous paragraphs, and then consider the rest as a perturbation δ_M. Then, we can define an analogous filtration using the multidegree of the modules composing the m-multicomplex.

Definition 2.2. In $M_{j_0,...,j_m}$, and for each generator σ, we put $J_\sigma := (j_1, ..., j_m)$. Then $F_{T^m_P}$ is defined as the free $\mathbb{Z}$-module generated by the $\sigma \in M_*$ such that $J_\sigma \in T^m_P$. If for every $d_{i_0,...,i_{m-1}}$ in δ_M we have $i_l \geq 1$, then the filtration is well defined.

Suppose we have effective homology for a multicomplex $(M_*, d_\otimes)$, $M_* \Longleftarrow DM_* \Rightarrow EM_*$. Then we want to know if we have also effective homology and a well-defined filtration for the perturbed chain complex $(M_*, d_\otimes + \delta_M)$, and if we obtain a similar spectral system.

Theorem 2.3. *Let $(M_*, d_\otimes + \delta_M)$ be a bounded m-multicomplex such that $i_j \geq 2$ for every $d_{i_0,\ldots,i_{m-1}}$ in δ_M and every $j = 0, \ldots, m-1$. Suppose that we have effective homology for the complex $(M, d_\otimes)$ such that the maps f and g of all the reductions maintain all the indexes of the multicomplex, whereas all h are a sum of maps such that each of them raises the sum of the k rightmost indexes in at most one unit, for $1 \leq k \leq m$. Then:*

1) *We have effective homology for the complex $(M, d_\otimes + \delta_M)$.*
2) *There are well defined spectral systems, associated to the generalized filtration F, and those on M_* and EM_* are isomorphic from the 2-page.*

Finally, we have a generalization for multicomplexes that are tensor products of chain complexes, obtaining a formula for the 2-page.

Theorem 2.4. *Let $M_* = (C^0_* \otimes C^1_* \otimes \ldots \otimes C^m_*, d_\otimes + \delta_M)$ be a bounded m-multicomplex such that the multidegree is given by the degrees of the tensor product. If the hypotheses of the previous theorem are satisfied, then the 2-page of the spectral system has the form:*

$$S_n(P; m) = H_{p_m}(C^m; H_{p_{m-1}}(C^{m-1}; \ldots H_{p_1}(C^1; H_{p_0}(C^0)),$$

with $P := (p_1, \ldots, p_m) \in \mathbb{Z}^m$ and $p_0 := n - p_1 - \ldots - p_m$.

Our results are being implemented as part of a new module for the Kenzo system, and will be available at: `https://github.com/DanielMT1997/Kenzo-external-modules`.

References

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

[2] A. Guidolin and A. Romero. Computing higher Leray–Serre spectral sequences of towers of fibrations, *Foundations of Computational Mathematics*, 21:1023–1074, 2021.

[3] A. Guidolin and A. Romero. Effective computation of generalized spectral sequences, *Proceedings of the 2018 ACM on International Symposium on Symbolic and Algebraic Computation*, 183–190, 2018.

[4] B. Matschke. Successive spectral sequences, to appear in Transactions of the AMS, 2022.

[5] D. Miguel, A. Guidolin, A. Romero and J. Rubio. Effective spectral systems relating Serre and Eilenberg–Moore spectral sequences, to appear in Journal of Symbolic Computation, 2022.

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

[7] J. Rubio and F. Sergeraert. Constructive Homological Algebra and Applications. Preprint `http://arxiv.org/abs/1208.3816`, 2006.

[8] F. Sergeraert. The computability problem in Algebraic Topology. *Advances in Mathematics*, 104(1):1–29, 1994.

[9] C. T. C. Wall, Resolutions for extensions of groups. *Mathematical Proceedings of the Cambridge Philosophical Society*, 57(2):251–255, 1961.

Universidad de La Rioja
Email address: `damigutr@unirioja.es`

KTH Royal Institute of Technology
Email address: `guidolin@kth.se`

Universidad de La Rioja
Email address: `ana.romero@unirioja.es`

Universidad de La Rioja
Email address: `julio.rubio@unirioja.es`

EFFECTIVE COMPUTATION OF THE GENERAL COMPONENT OF THE JET SCHEME

MARIO MORÁN CAÑÓN AND JULIEN SEBAG

Abstract. Let k be a perfect field. Let X be an integral k-variety. Let $m \in \mathbf{N}$. We study, from the theoretical and computational points of view, the component $\mathscr{G}_m(X)$ of the jet scheme $\mathscr{L}_m(X)$ defined to be the Zariski closure of the set of truncated arcs with a regular base-point. When $\mathrm{char}(k) = 0$ and X is a weighted homogeneous plane curve singularity, we provide a Gröbner basis of the ideal $\mathscr{N}_1(X)$ defining $\mathscr{G}_1(X)$ as a reduced closed subscheme of $\mathscr{L}_1(X)$. More generally, we prove that $\mathscr{G}_m(X)$ can be described from any smooth birational model of X. When X is supposed to be affine embedded in $\mathbf{A}_k^N$, this description provides an algorithm, valid for fields of arbitrary characteristic, which computes a Gröbner basis of a presentation of $\mathscr{G}_m(X)$ in $\mathbf{A}_k^{(m+1)N}$ from the datum of a given explicit smooth affine birational model of X. We finally present some applications.

Introduction

Let k be a perfect field. Let X be a k-variety, i.e., a k-scheme of finite type. For every element $m \in \mathbf{N} \cup \{\infty\}$, we define the *jet scheme* $\mathscr{L}_m(X)$ of level $m \in \mathbf{N}$ and the *arc scheme* $\mathscr{L}_\infty(X)$ associated with X by the functorial property

$$\mathrm{Hom}_{\mathrm{Sch}_k}(\mathrm{Spec}(A), \mathscr{L}_m(X)) \cong \mathrm{Hom}_{\mathrm{Sch}_k}(\mathrm{Spec}(A[[T]]/\langle T^{m+1}\rangle), X)$$

for every k-algebra A, and with the convention that $A[[T]]/\langle T^{m+1}\rangle = A[[T]]$ when $m = \infty$. When m runs over $\mathbf{N}$, the m-jet schemes, together with the morphisms $\theta^m_{n,X}$ induced by the projections $k[[T]]/\langle T^m\rangle \to k[[T]]/\langle T^n\rangle$, with $m \geq n$, form a projective system of k-schemes whose limit exists in Sch_k and coincides with the arc scheme of X. Let $\theta_{m,X} : \mathscr{L}_\infty(X) \to \mathscr{L}_m(X)$ be the canonical morphism of k-schemes. Note that $\theta^1_{0,X}$ canonically is the *tangent bundle* defined from the tangent space $T_X := \mathscr{L}_1(X) \cong \mathrm{Spec}(\Omega^1_{X/k})$ of X to X.

For $n \in \mathbf{N}$, $m \in \mathbf{N} \cup \{\infty\}$ we denote $k[x_1, \ldots, x_n]_m := k[(x_{i,j}); 1 \leq i \leq n, 0 \leq j \leq m]$ which is a $k[x_1, \ldots, x_n]$-module via the identification of $k[x_1, \ldots, x_n]_0$ and $k[x_1, \ldots, x_n]$. For every $f \in k[x_1, \ldots, x_n]$, there exists a unique family $(f_s)_{0 \leq s \leq m}$ of elements in $k[x_1, \ldots, x_n]_m$ such that the following equality holds in the ring $k[x_1, \ldots, x_n]_m[[t]]$:

$$f\left(\left(\sum_{j=0}^{m} x_{i,j} t^j\right)_{0 \leq i \leq n}\right) = \sum_{s=0}^{m} f_s\left((x_{i,j})_{\substack{0 \leq i \leq n \\ 0 \leq j \leq s}}\right) t^s \pmod{t^{m+1}}. \tag{1}$$

Let X be an affine k-variety such that $\mathcal{O}(X) = k[x_1, \ldots, x_n]/I$. We define the ideal I_m of the ring $k[x_1, \ldots, x_n]_m$ to be $I_m := \langle f_s : f \in I,\ 0 \leq s \leq m\rangle$. Then [1, Ch. 3, 2.3.5 and example 3.3.4] ensure that $\mathscr{L}_m(X) = \mathrm{Spec}(k[x_1, \ldots, x_n]_m/I_m)$.

The talk at the EACA 2022 meeting was given by the first named author.

Contents

Let $m \in \mathbf{N}$. If X is smooth over k, then the morphism $\theta^m_{0,X}$ is an affine bundle with fiber $\mathbf{A}_k^{m\dim(X)}$ (see [1, Ch. 3, Prop. 3.7.5]). Hence, if besides the k-variety X is assumed to be integral, then the jet scheme $\mathscr{L}_m(X)$ is also smooth and integral. For any integral k-variety X, the picture is more complicated. The reduced closed subscheme of $\mathscr{L}_m(X)$

$$\mathscr{G}_m(X) := \overline{(\theta^m_{0,X})^{-1}(\mathrm{Reg}(X))} = \overline{\mathscr{L}_m(\mathrm{Reg}(X))}.$$

is an irreducible component of $\mathscr{L}_m(X)$ with dimension $(m+1)\dim(X)$, called the *general component* of $\mathscr{L}_m(X)$. The possible other irreducible components of $\mathscr{L}_m(X)$ dominate $\mathrm{Sing}(X)$. The general component of a jet scheme is connected to the geometry of the base variety X; indeed it plays a role in different situations (see section 3). Given an affine k-variety $X = \mathrm{Spec}(k[x_1,\dots,x_n]/I)$, our aim is to present some methods to describe, from the theoretical and effective points of view, the prime ideal $\mathscr{N}_m(X)$ of $k[x_1,\dots,x_n]_m$ defining $\mathscr{G}_m(X)$ as a reduced closed subscheme of $\mathscr{L}_m(\mathbf{A}^n_k)$.

1. The general component of an affine plane curve defined by a homogeneous or weighted homogeneous polynomial

Let k be a field of characteristic zero. In [4], we provide theoretically a Gröbner basis (for a specific lexicographic monomial order) of $\mathscr{N}_m(X)$, for X an integral plane k-curve defined by a homogeneous or weighted homogeneous polynomial.

1.1. Let us consider the k-derivation D of $k[x,y]_1$ given by $D := x_1\partial_{x_0} + y_1\partial_{y_0}$. We denote by D^i the i-th iterate of D.

Theorem 1.1. *Let k be a field of characteristic 0. Let $X = \mathrm{Spec}(k[x,y]/\langle f\rangle)$ be an integral curve defined by a homogeneous polynomial $f \in k[x,y] = k[x,y]_0$ different from x and y. The family formed by f, $y_1x_0 - y_0x_1$ and $D^i(f)/i$ for every integer $i \in \{1,\dots,\deg(f)\}$ is a Gröbner basis of the ideal $\mathscr{N}_1(X)$ for the monomial order $y_1 >_{\mathrm{lex}} y_0 >_{\mathrm{lex}} x_1 >_{\mathrm{lex}} x_0$ in $k[x,y]_1$.*

Note that if $f = x$ (analogously for $f = y$) then X is smooth and $\mathscr{N}_1(X) = \langle f\rangle_1 = \langle x_0, x_1\rangle$.

1.2. Let $f \in k[x,y]$ be a reduced polynomial. We say that f is *weighted homogeneous* of weight (w_1,w_2,w) if we have, in the polynomial ring $k[x,y][t]$, the equality $f(t^{w_1}x, t^{w_2}y) = t^w f(x,y)$. If the field k is algebraically closed, this is equivalent to the existence of a k-automorphism σ of the ring $k[x,y]$, an integer $\ell \geq 1$, a pair of coprime integers (r,s) with $r \geq s$, and $\lambda_1,\dots,\lambda_\ell \in k^\times$ such that $\sigma(f) = x^\varepsilon y^{\varepsilon'}\prod_{i=1}^{\ell} x^r - \lambda_i y^s$ with $\varepsilon,\varepsilon' \in \{0,1\}$.

In this setting, we set $\widetilde{D}_{-1} := \widetilde{D}_{\lambda_i,-1} := sy_1x_0 - ry_0x_1$ and $\widetilde{D}_{\lambda_i,j_i} := \lambda_i s^{j_i} y_0^{s-j_i} y_1^{j_i} - r^{j_i} x_0^{r-j_i} x_1^{j_i}$, where $j_i \in \{0,\dots,s\}$. For every $i \in \{1,\dots,\ell\}$, if $j_i \in \{-1,\dots,s\}$, we denote

$$\widetilde{D}_{j_1,\dots,j_\ell} := \widetilde{D}_{\lambda_1,j_1}\cdots\widetilde{D}_{\lambda_t,j_\ell}.$$

Theorem 1.2. *Let k be a field of characteristic zero. Let $X = \mathrm{Spec}(k[x,y]/\langle f\rangle)$ be an integral k-curve defined by a weighted homogeneous polynomial $f \in k[x,y]$. Let $\overline{k}$ be an algebraic closure of k and $(e_\lambda)_{\lambda\in\Lambda}$ a basis of the k-vector space $\overline{k}$. With the preceding notation, we assume that in $\overline{k}[x,y]$, we can write $f = x^\varepsilon y^{\varepsilon'}\prod_{i=1}^{\ell} x^r - \lambda_i y^s$ with $\varepsilon,\varepsilon' \in \{0,1\}$. We consider the family of elements of $\overline{k}[x,y]_1$:*

$$\mathfrak{B} = \{\tilde{D}_{-1}, x_{h_1}^{\varepsilon} y_{h_2}^{\varepsilon'} \widetilde{D}_{j_1,\dots,j_\ell} \ :\ j_i \in \{-1,\dots,s\}, i \in \{1,\dots,\ell\}, h_1,h_2 \in \{0,1\}\}.$$

Then, the set $\mathfrak{C} = \{P_\lambda \ :\ P = \sum_{\lambda\in\Lambda} P_\lambda e_\lambda, P \in \mathfrak{B}\}$ is a Gröbner basis of $\mathscr{N}_1(X)$ for the monomial order $y_1 >_{\mathrm{lex}} y_0 >_{\mathrm{lex}} x_1 >_{\mathrm{lex}} x_0$ in $k[x,y]_1$.

2. Algorithms for computing the general component

In general, if the variety X does not satisfy the assumptions in theorems 1.1 or 1.2, or if $m > 1$, we do not know an explicit presentation of $\mathscr{N}_m(X)$. In [5], for any integral variety X defined over a perfect field k, we obtain a description of $\mathscr{G}_m(X)$ in terms of any smooth birational model of X. Using this, we provide two algorithms for computing $\mathscr{N}_m(X)$.

Theorem 2.1. *Let k be a perfect field. Let $m \geq 1$ be an integer. Let X, X' be integral k-varieties. We assume that X' is smooth over k. Let $h : X' \to X$ be a birational morphism. We denote by $h_m : \mathscr{L}_m(X') \to \mathscr{L}_m(X)$ the canonical morphism induced by h. Then,*

$$\mathscr{G}_m(X) = \overline{\theta_{m,X}(\mathscr{L}_\infty(X) \setminus \mathscr{L}_\infty(\mathrm{Sing}(X)))} = \overline{h_m(\mathscr{L}_m(X'))}.$$

In particular, if the arc scheme $\mathscr{L}_\infty(X)$ is irreducible, then the general component $\mathscr{G}_m(X)$ coincides with the Zariski closure of the image of $\mathscr{L}_\infty(X)$ by $\theta_{m,X}$.

The k-variety X' being smooth, $\mathscr{L}_m(X')$ also is; in particular it is reduced. Hence $\mathscr{G}_m(X)$ is the scheme-theoretic image of h_m, which is quasi-compact. This proves the following result.

Corollary 2.2. *Let k be a perfect field and $m \geq 1$ be an integer. Let X be an integral affine k-variety with $\mathcal{O}(X) = k[x_1, \ldots, x_n]/I$. Let X' be a smooth affine variety and $h : X' \to X$ be a birational morphism. We denote by $h_m : \mathscr{L}_m(X') \to \mathscr{L}_m(X)$ the canonical morphism induced by h, by $\pi_m : k[x_1, \ldots, x_n]_m \to k[x_1, \ldots, x_n]_m/I_m$ the canonical morphism and by $h_m^\sharp : \mathcal{O}(\mathscr{L}_m(X)) \to \mathcal{O}(\mathscr{L}_m(X'))$ the morphism of k-algebras induced by h_m. Then we have*

$$\mathscr{N}_m(X) = \mathrm{Ker}(h_m^\sharp \circ \pi_m).$$

All the objects involved in the corollary can be effectively computed. Thus we obtain the following algorithm.

Algorithm 1: Computation of $\mathscr{N}_m(X)$ from an arbitrary smooth birational model.

Input : Presentations of $\mathcal{O}(X) \cong k[x_1, \ldots, x_n]/I$ and $\mathcal{O}(X') \cong k[y_1, \ldots, y_\ell]/J$, the morphism $h^\sharp : \mathcal{O}(X) \to \mathcal{O}(X')$, $m \in \mathbf{N}$.
Output : the ideal $\mathscr{N}_m(X)$ of $k[x_1, \ldots, x_n]_m$.

Compute $\mathcal{O}(\mathscr{L}_m(X)) \cong k[x_1, \ldots, x_n]_m/I_m$ and $\mathcal{O}(\mathscr{L}_m(X')) \cong k[y_1, \ldots, y_\ell]_m/J_m$ (see (1)).
Compute the induced morphism $h_m^\sharp : k[x_1, \ldots, x_n]_m \to k[y_1, \ldots, y_\ell]_m/J_m$.
return $\mathrm{Ker}(h_m^\sharp)$

2.1. There are various ways of obtaining smooth birational models of an integral variety (e.g., normalization for curves, resolution of singularities). Note that the inclusion $U \hookrightarrow X$ satisfies the required properties, for every open subscheme U of $\mathrm{Reg}(X)$. In particular, we can choose $H \in k[x_1, \ldots, x_n]$ such that $U = \{H \neq 0\} \subset \mathrm{Reg}(X)$ and in this case $\mathscr{N}_m(X) = (I_m : H^\infty)$ (see [5] for justification and references). The saturation being computable, we obtain another algorithm for computing $\mathscr{N}_m(X)$ (see [3] for a first version).

Algorithm 2: Computation of $\mathscr{N}_m(X)$ using a standard open subscheme of $\mathrm{Reg}(X)$.

Input : A presentation of $\mathcal{O}(X) \cong k[x_1, \ldots, x_n]/I$, $m \in \mathbf{N}$.
Output : the ideal $\mathscr{N}_m(X)$ of $k[x_1, \ldots, x_n]_m$.

Compute the Jacobian ideal Jac of I; choose $H \in Jac \setminus I$.
Compute $\mathcal{O}(\mathscr{L}_m(X)) \cong k[x_1, \ldots, x_n]_m/I_m$ using (1).
return $(I_m : H^\infty)$, here H is seen as an element of $k[x_1, \ldots, x_n]_m$.

3. Applications

3.1. Let X be an integral k-variety, $m \in \mathbf{N}$. By the very definition of $\mathscr{G}_m(X)$ we deduce that $\mathscr{L}_m(X)$ is irreducible if and only if $\mathscr{G}_m(X) = \mathscr{L}_m(X)$, i.e., $\mathscr{N}_m(X) = I_m$ if X is affine. There is a connection between the topology of the jet schemes and the singularities of X (see the theorem of Mustaţă below) which may justify the interest in understanding $\mathscr{G}_m(X)$.

Theorem 3.1 ([6, Theorem 0.1])**.** *Let k be an algebraically closed field of characteristic zero and X be locally a complete intersection k-variety. Then the variety X only has rational singularities if and only if the schemes $\mathscr{L}_m(X)$ are irreducible for every integer $m \geq 1$.*

3.2. If the arc scheme $\mathscr{L}_\infty(X)$ is assumed to be irreducible (e.g., if $\dim(X) = 1$ by [1, Ch. 3, Lemma 4.3.1]; or $\mathrm{char}(k) = 0$ by the Kolchin irreducibility theorem [2, IV/6/Exercise 3d]) then theorem 2.1 implies that $\mathscr{N}_m(X) = \sqrt{I_\infty} \cap k[x_1, \ldots, x_n]_m$. Hence our study provides a description of the nilpotent functions of the arc scheme. In the spirit of theorem 3.1, we may ask about a possible relation of the reducedness of $\mathscr{L}_\infty(X)$ and the singularities of X.

3.3. For $X = \mathrm{Spec}(k[x,y]/\langle f \rangle)$ an integral plane curve and $m = 1$ there are some implications of our study in terms of differential operators. Let $\mathscr{D}$ be the set of differential operators of $k[x,y]$ and V_{d-1} be the left $k[x,y]$-submodule of $\mathscr{D}$ generated by the *homogeneous* differential operators $D = \sum_{i=0}^{d} a_i \partial_{x_1}^i \partial_{x_2}^{d-i}$ (here $a_i \in k[x,y]$) such that $D(f^d) \in \langle f \rangle$. We consider the morphism of left $k[x,y]$-modules $(\cdot)^\sharp \colon k[x,y]_1 \to \mathscr{D}$ defined by $\sum_{i=0}^{d} a_i x_1^i y_1^{d-i} \mapsto \sum_{i=0}^{d} (-1)^i a_i \partial_y^i \partial_x^{d-i}$. Let $\mathscr{N}_1^d(X)$ be the set of homogeneous elements of $\mathscr{N}_1(X)$ of degree d in x_1, y_1. The following result appears in [7] when $\mathrm{char}(k) = 0$ and in [5] under this form. It implies that we can use our study to determine V_{d-1}.

Theorem 3.2. *Let k be a perfect field. Let $d \geq 1$ be an integer such that $d!$ is prime to the characteristic exponent of k. The morphism $(\cdot)_d^\sharp : \mathscr{N}_1^d(X) \to V_{d-1}$ induced by restriction of $(\cdot)^\sharp$ is an isomorphism of left $k[x,y]$-modules.*

References

[1] Antoine Chambert-Loir, Johannes Nicaise and Julien Sebag, *Motivic integration*, Progress in Mathematics, vol 325, Birkhäuser/Springer, New York, 2018.

[2] E. R. Kolchin, *Differential algebra and algebraic groups*, Academic Press, New York-London, 1973, Pure and Applied Mathematics, Vol. 54.

[3] Kodjo Kpognon, *Singularités des courbes planes, module des dérivations et schéma des arcs*, PhD Thesis, Université de Rennes 1, 2014.

[4] Mario Morán Cañón and Julien Sebag, *On the tangent space of a weighted homogeneous plane curve singularity*, J. Korean Math. Soc. **57** (2020), no. 1, 145-169.

[5] Mario Morán Cañón and Julien Sebag, *Two algorithms for computing the general component of jet scheme and applications*, Journal of Symbolic Computation **113** (2022), 74-96.

[6] Mircea Mustaţă, *Jet schemes of locally complete intersection canonical singularities*, Invent. Math. **145** (2001), 397-424. With an appendix by David Eisenbud and Edward Frenkel.

[7] Julien Sebag, *On logarithmic differential operators and equations in the plane*, Illinois J. Math. **62** (2018), no. 1-4 215-224.

Department of Mathematics, University of Oklahoma, 601 Elm Ave., Norman, OK 73019 (USA).
Email address: mariomc@ou.edu

Institut de recherche mathématique de Rennes, UMR 6625 du CNRS, Université de Rennes 1, Campus de Beaulieu, 35042 Rennes cedex (France).
Email address: julien.sebag@univ-rennes1.fr

ON THE GENERATORS OF THE VALUE SEMIGROUP AT INFINITY ASSOCIATED TO A CURVE WITH ONLY ONE PLACE AT INFINITY

CARLOS-JESÚS MORENO-ÁVILA AND JULIO-JOSÉ MOYANO-FERNÁNDEZ

Abstract. Let C be a curve with only one place at infinity, and let $S_{C,\infty}$ be its semigroup at infinity. It is known that this semigroup is generated by a δ-sequence in $\mathbf{N}_{>0}$. In this work we study the family of δ-sequences which generate the same semigroup $S_{C,\infty}$ at infinity. We also introduce the minimal δ-sequences as those with the least length among all the δ-sequences generating the same semigroup at infinity. This is based on a joint work in progress with C. Galindo and F. Monserrat.

Preliminaries

We set the following notation: write $\mathbb{N}$ for the set of nonnegative integers. For $n \in \mathbb{N}$, we will write $\mathbb{N}_{>n}$ for the infinite subset $\{n+1, n+2, \ldots\} \subseteq \mathbb{N}$. Moreover, set $[n] := \{1, \ldots, n\}$ and $[0, n] := \{0, 1, \ldots, n\}$.

Let k be a field, and let $\overline{k}$ be the algebraic closure of k. Set $\mathbb{P}^2 = \mathbb{P}^2_k$ for the projective plane over k. Let L be the line at infinity in the compactification of the affine plane to $\mathbb{P}^2$. An absolutely irreducible curve C of $\mathbb{P}^2$ (i.e. irreducible as a curve in $\mathbb{P}^2_{\overline{k}}$) is said to *have only one place at infinity* if the intersection $C \cap L$ is a single point p and C has only one rational (i.e. defined over k) branch at p. The point p is then said to be the point at infinity.

The geometry around the point at infinity of a curve C as above was first studied by Abhyankar and Moh [1] by means of what they called the semigroup at infinity: let K be the quotient field of the local ring $\mathcal{O}_{C,p}$ associated with a curve C with only one place at infinity at p. For convenience, we will fix homogeneous coordinates $(X : Y : Z)$ on $\mathbb{P}^2$, and we can assume without loss of generality that $p = (1 : 0 : 0)$. The equation $Z = 0$ will describe the line at infinity. Set affine coordinates (x, y) in the chart $Z \neq 0$, as well as affine coordinates $(u = y/x, v = 1/x)$ around the point at infinity. We shall assume that the curve C is defined by a monic polynomial $f(x, y) \in k[x][y]$ in the indeterminate y with coefficients in $k[x]$.

Since the germ of C at p defines a discrete valuation $\nu := \nu_{C,p}$ on K, i.e. the valuation associated to the only valuation ring R_ν not containing the affine k-algebra for the chart $Z \neq 0$ of C and dominating $\mathcal{O}_{C,p}$, we define:

The first author was supported by the Margarita Salas postdoctoral contract MGS/2021/14(UP2021-021) financed by the European Union-NextGenerationEU.

The authors were partially supported by MCIN/AEI/10.13039/501100011033 and by "ERDF – A way of making Europe", grants PGC2018-096446-B-C21, PGC2018-096446-B-C22 and RED2018-102583-T, as well as by Universitat Jaume I, grant UJI-B2021-02.

The talk at the EACA 2022 meeting was given by the second author.

Definition 0.1. Let C be a curve with one place at infinity given by p. The *semigroup at infinity* of C is the additive sub-semigroup of $\mathbb{N}$

$$S_{C,\infty} := \{-\nu(z) : z \in \mathcal{O}_C(C \setminus \{p\})\}$$

The semigroup $S_{C,\infty}$ is numerical, i.e. it has a finite complement in $\mathbb{N}$; more precisely:

Definition 0.2. For $g \geq 0$, let $\Delta = (\delta_i)_{i=0}^{g}$ be a sequence in $\mathbb{N}_{>0}^{g+1}$. We say that Δ is a δ-sequence in $\mathbb{N}_{>0}$ (or simply a δ-sequence) if the following conditions hold:

(1) If $d_i = \gcd(\delta_0, \delta_1, \ldots, \delta_{i-1})$, for $1 \leq i \leq g+1$, and $n_i = d_i/d_{i+1}, 1 \leq i \leq g$, then $d_{g+1} = 1$ and $n_i > 1$ for every $i \in [g]$.
(2) For $i \in [g]$, the integer $n_i\delta_i$ belongs to the semigroup $\mathbb{N}\delta_0 + \mathbb{N}\delta_1 + \cdots + \mathbb{N}\delta_{i-1}$.
(3) $\delta_0 > \delta_1$ and $\delta_i < n_{i-1}\delta_{i-1}$ for every $i \in [g]$.

We will denote by $\delta_i(\Delta)$ the ith generator of the δ-sequence Δ, and we will drop Δ if no confusion arises. The numerical semigroup generated by a δ-sequence Δ will be denoted by S_Δ. The fact that δ-sequences in $\mathbb{N}_{>0}$ are indeed generators of the semigroup $S_{C,\infty}$ is due to Abhyankar and Moh [1]. Following their construction, the element δ_0 acquires a geometric meaning: this is the degree of C. Moreover, the sequence $n(\Delta) = \{n_i(\Delta)\}_{i=1}^{g}$ will be called the n-sequence of Δ.

In this paper, we present an extended abstract of a work in progress with C. Galindo and F. Monserrat [2], in which among other issues, we inquire concerning the combinatorial properties of the δ-sequences which allow us to understand the singularity at infinity. In particular, given a curve C as above, we look for *minimal* δ-sequences, in the sense that they have the least possible length, but generate the same semigroup at infinity $S_{C,\infty}$; they are interesting since no minimal set of generators is known. For further reading, we refer to Galindo and Monserrat [3, 4] and references therein.

1. δ-sequences and their refinements

The δ-sequences $\mathbb{N}_{>0}^{g+1}$ generating $S_{C,\infty}$ are of finite length and they are not unique: in fact, there exist infinitely many δ-sequences of different lengths generating the same semigroup at infinity. Geometrically, this means that it is possible to find different curves C having the same semigroup at infinity but with germs at p which are not equisingular, i.e. which have different value semigroups at p.

The aim of this short note is to give a flavour of the task of finding (finitely many) significant families of δ-sequences generating the same semigroup at infinity. First of all, we deal with a technical result.

Proposition 1.1. *Let $g \geq 0$ be an integer. A sequence $\Delta = (\delta_i)_{i=0}^{g}$ in $\mathbb{N}_{>0}^{g+1}$ is a δ-sequence if and only if there exists another sequence $(n_j)_{j=1}^{g}$ in $\mathbb{N}_{>0}^{g+1}$ with $n_j > 1$ for all j, such that*

$$\delta_i = a_i \prod_{j=i+1}^{g} n_j,$$

where $n_0 = a_0 = 1$, $\gcd(n_i, a_i) = 1$, $a_i < n_i n_{i-1} a_{i-1}$ for $1 \leq i \leq g$ (by convention, we set $\prod_{j=i+1}^{g} n_j = 1$ if $i = g$) and, when $i \geq 2$, the integer a_i belongs to the semigroup spanned by the values a_{i-1} and $\prod_{\ell+1 \leq j \leq i-1} n_j a_\ell$, for $\ell = 0, 1, \ldots, i-2$.

As a consequence we obtain the following.

Corollary 1.2. *Let δ_0 be a positive integer. There exist finitely many δ-sequences Δ whose first element is δ_0.*

From Proposition 1.1, we deduce that there is no δ-sequence with the same δ_0 whose length is larger than 1 plus the number of prime factors of δ_0.

Given a δ-sequence Δ, we want to investigate under which conditions we can add elements to Δ in such a way that the nature of being δ-sequence generating the same numerical semigroup is preserved. With this aim in mind, we introduce the concept of refinement of a δ-sequence in $\mathbb{N}_{>0}$.

Definition 1.3. Let $\Delta = (\delta_i)_{i=0}^{g}$, $\Delta' = (\delta'_i)_{i=0}^{g'}$ be δ-sequences in $\mathbb{N}_{>0}$. The sequence Δ' is said to be a *refinement* of Δ if there exists a subset $\{i_0, i_1, \ldots, i_g\}$ of pairwise different elements in $[0, g']$ with $i_0 < i_1 < \cdots < i_g$ and such that $\delta'_{i_j} = \delta_j$ for every $j \in [0, g]$. The cardinality of the set $\Delta' \setminus \Delta$ is called to be the *order of refinement* of Δ' with respect to Δ.

For instance, $\Delta' = (108, 72, 24, 54, 26, 13)$ is a refinement of order 2 of $\Delta = (108, 24, 54, 13)$. By looking at the n-sequences $n(\Delta') = (3, 3, 2, 3, 2)$ resp. $n(\Delta) = (9, 2, 6) = (3 \cdot 3, 2, 3 \cdot 2)$, the word "refinement" acquires its meaning: the former n-sequence refines the latter, since $n(\Delta)$ concentrates factors of $n(\Delta')$.

2. Minimal δ-sequences

In this section we introduce the definition of minimal δ-sequence in $\mathbb{N}_{>0}$. They are a sort of minimal elements in the families of δ-sequences generating $S_{C,\infty}$ which may be thought as representatives of this semigroup at infinity. The idea is to fix a δ-sequence Δ in $\mathbb{N}_{>0}$, and consider nested sequences of δ-sequences containing Δ and generating the same semigroup. The minimal δ-sequence will be those of least cardinality.

Definition 2.1. Let Δ be a δ-sequence in $\mathbb{N}_{>0}$ and S_Δ the semigroup spanned by Δ. The sequence Δ is said to be a *minimal δ-sequence in* $\mathbb{N}_{>0}$ if there is no δ-sequence Δ' in $\mathbb{N}_{>0}$ such that Δ is a refinement of Δ' of order 1 and $S_{\Delta'} = S_\Delta$.

Remark 2.2. Note that from a δ-sequence in $\mathbb{N}_{>0}$, one can find other minimal δ-sequences only by permuting their elements. For instance $(15, 12, 10)$, $(15, 10, 12)$, $(12, 10, 15)$ are minimal δ-sequences generating the same semigroup.

Definition 2.3. A *nested family of δ-sequences in* $\mathbb{N}_{>0}$ is a finite or infinite sequence $\mathcal{D} = \{\Delta_i\}_{i \in I}$ of δ-sequences in $\mathbb{N}_{>0}$ such that Δ_{i+1} is a refinement of order 1 of Δ_i for every index $i \in I$.

For a fixed curve C as above with only one place at infinity, there is an infinite number of curves C' with only one place at infinity whose equisingularity class at p is different from C and both semigroups at infinity $S_{C,\infty}$ and $S_{C',\infty}$ coincide: this is the content of Theorem 2.4. However, as we have seen, that number is finite whenever we restrict ourselves to curves C' whose degree is less than (or equal to) the degree of C.

Theorem 2.4. *Let $\Delta = \{\delta_0, \delta_1, \ldots, \delta_g\}$ be a δ-sequence in $\mathbb{N}_{>0}$. Then there exists a nested infinite family $\mathcal{D} = \{\Delta_i\}_{i \geq 0}$ of δ-sequences in $\mathbb{N}_{>0}$ such that $\Delta_0 = \Delta$ and $S_{\Delta_i} = S_\Delta$ for*

every index i. Therefore, if C is a curve with only one place at infinite such that $S_\Delta = S_{C,\infty}$, then there exists a curve C' as above such that $S_{C',\infty} = S_\Delta$, and whose attached δ-sequence is as large as we desire.

Theorem 2.4 does not hold if multiples of the value δ_0 are not allowed.

Theorem 2.5. *Let $\Delta := \Delta_0$ be a minimal δ-sequence in $\mathbb{N}_{>0}$. Then there exist finitely many nested families $\mathcal{D} := \{\Delta_i\}_{i\geq 0}$ of δ-sequences in $\mathbb{N}_{>0}$ such that $\delta_0(\Delta_i)$ is not a multiple of $\delta_0(\Delta_{i-1})$, i.e. $\delta_0(\Delta_i) \neq a\delta_0(\Delta_{i-1})$ for $a \neq 1$, and $S_\Delta = S_{\Delta_i}$ for every $i \geq 0$. Furthermore, the cardinality of any family $\mathcal{D}$ is also finite.*

The following result enlarges the information on nested sequences given in the previous result, and allows us to give an algorithmic procedure to obtain a minimal δ-sequence from a δ-sequence in $\mathbb{N}_{>0}$.

Theorem 2.6. *Let $\Delta = \{\delta_0, \delta_1, \ldots, \delta_g\}$ be a δ-sequence in $\mathbb{N}_{>0}$, and let Δ_1 a refinement of Δ with $\Delta_1 \setminus \Delta = \{\delta\}$ and $S_\Delta = S_{\Delta_1}$. Then there exists an index $i_0 \in [0, g]$ such that $\delta = \ell\delta_{i_0}$, $\ell > 1$.*

Given a δ-sequence Δ, we can use the following algorithm for either, deciding that it is a minimal one, or computing a minimal one generating the same semigroup as Δ.

Algorithm 2.7. *Input:* A δ-sequence in $\mathbb{N}_{>0}$, say $\Delta = \{\delta_i\}_{i=0}^g$.

Output: A minimal δ-sequence A in $\mathbb{N}_{>0}$ that generates the semigroup S_Δ.

— Step 1: Set δ_{i_0} the minimum element in $A := \Delta$ and write $A' = \{\delta_{i_0}\}$.
— Step 2: Set δ_{i_1} the minimum element in $A \setminus A'$.
— Step 3: If δ_{i_1} is not a multiple of any element in $A \setminus \{\delta_{i_1}\}$, then we keep the same set A, set $A' = A' \cup \{\delta_{i_1}\}$ and go to Step 2. Otherwise, $A := A \setminus \{\delta_{i_1}\}$.
— Step 4: Check whether A is a δ-sequence in $\mathbb{N}_{>0}$. If this is not the case, $A = A \cup \{\delta_{i_1}\}$ and $A' = A' \cup \{\delta_{i_1}\}$.
— Step 5: Repeat the procedure until $A' = A$; after that, go to Step 6.
— Step 6: A is a minimal δ-sequence in $\mathbb{N}_{>0}$ with the same semigroup than Δ.

Clearly if the output is Δ, then it means that Δ is minimal.

References

[1] S. S. Abhyankar, T. T. Moh, Newton-Puiseux expansion and generalized Tschirnhausen transformation, *J. Reine Angew. Math.* **260** (1973), 47—83 and **261** (1973), 29–54.
[2] C. Galindo, F. Monserrat, C.J. Moreno-Ávila, J.J. Moyano-Fernández, On δ-sequences associated to a curve with only one place at infinity. Work in progress.
[3] C. Galindo, F. Monserrat, δ-sequences and evaluation codes defined by plane valuations at infinity, *Proc. London Math. Soc.* **98** (2009), 714–740.
[4] C. Galindo, F. Monserrat, The Abhyankar-Moh theorem for plane valuations at infinity. Journal of Algebra **374** (2013), 181–194.

Universitat Jaume I, Campus de Riu Sec, Departamento de Matemáticas & Institut Universitari de Matemàtiques i Aplicacions de Castelló, 12071, Castellón de la Plana, Spain
Email address: moyano@uji.es
Email address: cavila@uji.es

ALGEBRAIC ANALYSIS OF STABLE COHERENT SYSTEMS

P. PASCUAL-ORTIGOSA, R. IGLESIAS, AND E. SÁENZ-DE-CABEZÓN

Abstract. We define several notions of stability for coherent systems, and give two algebraic methods for computing the reliability of stable coherent systems. The approach we use is based on the algebraic approach to system reliability and uses Mayer-Vietoris trees and involutive bases as the main tools. We demonstrate that this approach is computationally efficient giving some computer experiments.

Introduction

Redundancy is one of the driving forces in the design of coherent systems. The balance between redundancy and cost optimization is a main criterion in the reliability-based design of these systems. A first strategy for the construction of redundant reliable systems is parallelization. A parallel system works whenever at least one of its components is working, and is therefore a demanding system in terms of resources. A less demanding alternative is k-out-of-n:G systems, which work whenever at least k of its n components are working (note that parallel systems are 1-out-of-n:G systems). k-out-of-n systems and their variants have been extensively studied and are ubiquitous in communication networks and industrial and applications [8, 16].

1. Fully stable, strongly stable and stable coherent systems

A system is a collection of components with different levels of performance. It is said to be*coherent* if the improvement of any component does not lead to a degrading of the system's performance. Let S be a coherent system with n components and let $\mathcal{F}_S$ (resp. $\overline{\mathcal{F}}_S$) the set of working states or paths of S (resp. minimal paths). We say that S is *fully stable* if for any path $m \in \mathcal{F}_S$, $m = (m_1, \ldots, m_n)$ and any component $i \in \{1, \ldots, n\}$ we have that $m - m_i + m_j = (m_1, \ldots, m_i - 1, \ldots, m_j + 1, \ldots, m_n)$ is also a path of S for any $i \neq j \in \{1, \ldots, n\}$. In the binary case the only fully stable systems are k-out-of-n systems.

The next two definitions relax the conditions of fully stable systems to describe two less demanding versions of stability. For these, we need to set a prevalence order among the components. In the next two definitions S is a coherent system with n components in which we have established a precedence ordering in the components according to some criterion like importance or efficiency, etc...

Definition 1.1. We say that S is *strongly stable* if for any path $m \in \mathcal{F}_S$, $m = (m_1, \ldots, m_n)$ and any component $i \in \{1, \ldots, n\}$ we have that $m - m_i + m_j = (m_1, \ldots, m_j + 1, \ldots, m_i - 1, \ldots, m_n)$ is also a path of S for any $i > j \in \{1, \ldots, n\}$.

The authors have been partially supported by grant PID2020-116641GB-100 funded by MCIN/AEI /10.13039/501100011033 (Spain).

The talk at the EACA 2022 meeting was given by the first author.

Definition 1.2. We say that S is *stable* if for any path $m \in \mathcal{F}_S$, $m = (m_1, \ldots, m_n)$ and the last working component i of m we have $m - m_i + m_j = (m_1, \ldots, m_j + 1, \ldots, m_i - 1, \ldots)$ is also a path of S for any $i > j \in \{1, \ldots, n\}$.

For any coherent system S we can define the stable and strongly stable closures of S as respectively the minimal stable and strongly stable systems whose set of paths contain the set of paths of S. Note that the fully stable closure of a system S is the k-out-of-n system, where k is the minimum length of any path of S.

2. Algebraic analysis of stable coherent systems

The algebraic approach to system reliability was initiated in [7] and developed in a series of papers including [11, 12, 13, 14]. The main idea of this approach is to associate a monomial ideal I_S (or a series of monomial ideal in the multi-state case) to a given coherent system S and compute the reliability of the system in terms of algebraic invariants of the ideal. The computation of the reliability amounts to computing the probability of the system of being in a working state, which in the algebraic formulation means being able to enumerate the monomials in the associated monomial ideal. Such an enumeration can be performed in two ways. One is to compute the numerator of the Hilbert series of I_S (in particular obtained as an alternated sum of the ranks of the modules in any free resolution of I_S so that we can also obtain bounds for the reliability), and the other way is to give a combinatorial disjoint decomposition of I_S. The first option constitutes an algebraic version of improved inclusion-exclusion formulas and bounds, cf. [3], while the second option is an algebraic variant of the Sum of Disjoint Products method [5, 16].

The case of stable coherent systems is particularly well suited to the algebraic approach. On the one hand, the ideal corresponding to a stable system is a stable ideal, for which an explicit formulation of their minimal free resolution is known [4], which makes the algebraic computation of the reliability of S very efficient in this case, using the Hilbert series of I_S. Furthermore, the support of the minimal free resolution is given by their Mayer-Vietoris trees, which makes this algorithm a good alternative for the computation of their Hilbert series [10].

For the reliability ideals of strongly stable systems, we can prove that their minimal generating set is already a Janet basis [6], and we know that from a Janet basis of a monomial ideal, we can read off a combinatorial disjoint decomposition of the ideal [15]. Hence this is an efficient approach in this case.

3. Computer Experiments

We use the `C++` class for algebraic computations implemented in `CoCoALib` [2] described in [1] to compute the reliability of some examples. First, we compute the reliability for several k-out-of-n systems and compare the sizes of their Mayer-Vietoris trees (i.e. the number of summands of the compact inclusion-exclusion formula given by the Hilbert series) and the sizes of their Janet bases (i.e. the number of summands in the algebraic Sum of Disjoint Products formula). Figure 1 shows that in binary k-out-of-n systems, as k increases with respect to n, the ratio between the size of the Janet basis of the ideal and the size of its Mayer-Vietoris tree (equiv. its minimal free resolution) increases. The Janet bases of these systems are much smaller than their Mayer-Vietoris trees (for n large and k small the

		k														
n		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
10	JB	10	45	120	210	252	210	120	45	10	1						
	MVT	1023	4097	7423	7937	5503	2561	799	161	19	1						
12	JB	12	66	220	495	792	924	792	495	220	66	12	1				
	MVT	4095	20481	47103	65537	61183	40193	18943	6401	1519	241	23	1				
14	JB	14	91	364	1001	2002	3003	3432	3003	2002	1001	364	91	14	1		
	MVT	16383	98305	274431	471041	553983	471041	297727	141569	50623	13441	2575	337	27	1		
16	JB	16	120	560	1820	4368	8008	11440	12870	11440	8008	4368	1820	560	120	16	1
	MVT	65535	458753	1507327	3080193	4374527	4571137	3629055	2228225	1066495	397825	114687	25089	4031	449	31	1

TABLE 1. Sizes of Janet bases and Mayer-Vietoris Trees for some binary k-out-of-n systems

difference is very significant). These sizes are presented in Table 1. The shaded region in Figure 1 indicates where the current implementations of Janet bases performs faster than the MVT algorithms in `CoCoALib`.

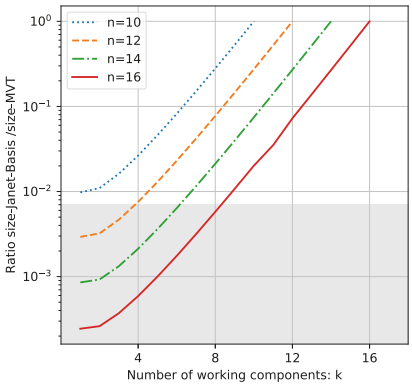


FIGURE 1. Ratios between the sizes of the Janet bases and Mayer-Vietoris Trees (equiv. minimal free resolutions) for several binary k-out-of-n systems

Our second example involves stable systems. Stable and strongly-stable ideals tend to have high Betti numbers for a given Hilbert function, while their involutive bases tend to be small. In particular, their Janet bases are given by the set of minimal monomial generators of the ideal. As an example, Figure 2 shows the number of generators and size of Mayer-Vietoris trees for all the 1819 strongly stable ideals in 10 variables with a Hilbert function $h = 6t+2$. The shaded dots indicate the region where the current implementations of Janet bases performs faster than the MVT algorithms in `CoCoALib`.

REFERENCES

[1] A. Bigatti, P. Pascual-Ortigosa and E. Sáenz-de-Cabezón, *A `C++` class for multi-state algebraic reliability computations*, Reliability Engineering & System Safety 213, 107751(2021)

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

[3] Dohmen, K., *Improved Bonferroni inequalities via abstract tubes*, Springer, 2003

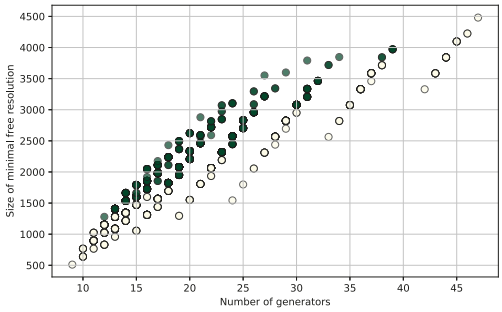


FIGURE 2. Sizes of minimal generating set vs. minimal free resolution for the strongly-stable ideals in ten variables with Hilbert polynomial $p = 6t+2$.

[4] S. Eliahou and M. Kervaire, *Minimal free resolutions of some monomial ideals*, Journal of Algebra, Vol. 129 (1990), pp. 1–25
[5] L. Fratta and U.G. Montanari, *A Boolean algebra method for computing the terminal reliability in a communication network*, IEEE Transactions on Circuit Theory, Vol.20 (1973), pp. 203–211
[6] V. Gerdt and Y. Blinkov, *Involutive bases of polynomial ideals*, Mathematics and Computers in Simulation, Vol. 45 (1998), pp. 519–542
[7] Giglio, B., Wynn, H. P., *Monomial ideals and the Scarf complex for coherent systems in reliability theory*, Annals of Statistics, Vol. 32 (2004), pp. 1289–1311
[8] W. Kuo and M. Z. Zuo, *Optimal reliability modelling*, Wiley and sons, 2002
[9] Pascual-Ortigosa, P., Sáenz-de-Cabezón, E., Wynn, H., *Algebraic reliability of multi-state k-out-of-n systems*, Probability in the Engineering and Informational Sciences, in press (2020), DOI: 10.1017/S0269964820000224
[10] Sáenz-de-Cabezón, E., *Multigraded Betti numbers without computing minimal free resolutions*, Appl. Alg. Eng. Commun. Comput., vol. 20 (2009), pp. 481–495.
[11] E. Sáenz-de-Cabezón and H.P. Wynn, *Betti numbers and minimal free resolutions for multi-state system reliability bounds*, Journal of Symbolic Computation 44 (2009), pp. 1311–1325.
[12] Sáenz-de-Cabezón, E., Wynn, H. P., *Mincut ideals of two-terminal networks*, Applicable Algebra Eng. Commun. Comput., vol. 21 (2010), pp. 443–457.
[13] Sáenz-de-Cabezón, E., Wynn, H. P., *Computational algebraic algorithms for the reliability of generalized k-out-of-n and related systems*, Math. Comput. Simulation, vol. 82, no. 1 (2011), pp. 68–78.
[14] E. Sáenz-de-Cabezón and H.P. Wynn, *Hilbert functions for design in reliability*, IEEE Transactions on Reliability, vol. 64, no. 1 (2015), pp. 83–93.
[15] W. M. Seiler, *A combinatorial approach to involution and δ-regularity II: Structure analysis of polynomial modules with Pommaret bases*, Applicable Algebra Eng. Commun. Comput., vol. 20 (2009), pp. 261–338.
[16] K. S. Trivedi and A. Bobbio, *Reliability and Availability Engineering*, Cambridge University Press, 2017.

Universidad de La Rioja
Email address: papasco@unirioja.es
Email address: rodrigo.iglesias@unirioja.es
Email address: esaenz-d@unirioja.es

CURVES OF CONSTANT WIDTH AND ZINDLER CURVES: DUALITY AND ALGEBRAIC EQUATIONS

DAVID ROCHERA

Abstract. The relationship between curves of constant width and Zindler curves with offsets and front track curves is described and generalized to non-convex shapes. A one-to-one correspondence between hedgehogs of constant width and standard generalized Zindler curves is provided in terms of a projective hedgehog. With this idea, given a family of projective hedgehogs defined by trigonometric polynomials as support functions, an explicit method to compute algebraic equations for the associated curves of constant width and Zindler curves is possible. This extends the methodology used by Rabinowitz and Martinez-Maure in particular constant width curves to generate a full family of algebraic equations, both of curves of constant width and Zindler curves.

Introduction

A planar convex body K is called of constant width if its width, defined as the distance between any pair of parallel supporting lines to K, is constant in any direction. The boundary of K is called a curve of constant width. There are many known non-circular examples of this kind of curve (see [5] for an introduction to the topic).

Zindler curves [9] are another kind of curve which is closely related to curves of constant width. The property that defines a Zindler curve is that all chords that cuts the curve perimeter (or area) into halves (namely, halving chords), have the same length. Zindler curves are also the boundaries of figures of constant density $1/2$ that float in water in equilibrium in any position [2].

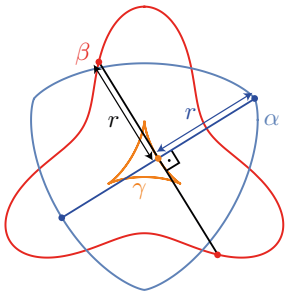


Figure 1. A curve α of constant width $2\,r$, its "dual" Zindler curve β and their associated middle hedgehog γ.

The author has been partially supported by the Spanish Ministry of Sciences, Innovation and Universities though a BCAM Severo Ochoa accreditation of excellence (SEV-2017-0718).

Contents

We know that there is a "duality" between curves of constant width and Zindler curves (see e.g. [5]), in the sense that, under some convexity assumptions, a right angle rotation of the constant width chord in the first case or the halving chord in the second case yields the other figure as described by the endpoints (see Figure 1). The locus of all these midpoints also determines another curve called the *middle hedgehog*, which is a projective hedgehog by construction.

The duality above can be described by offsets and front tracks. Offset curves are those which are at a constant distance from another in an orthogonal direction, while front wheel track curves are those which are found at a constant distance from another (the rear wheel track curve) in a tangential direction (see Figure 2).

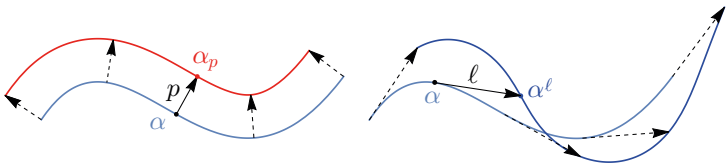


FIGURE 2. On the left, an offset α_p to a curve α at a distance p. On the right, the front wheel track curve α^ℓ to a rear wheel track curve α for a bicycle of length ℓ.

Thanks to these relations, this duality can be easily generalized to a one-to-one correspondence between hedgehogs of constant width and standard generalized Zindler curves can be proved (Theorem 1.3).

Rabinowitz asked in [6] for algebraic equations describing non-circular constant width curves. He found a quite complicated expression, and he asked if simpler expressions could be given. Recently, Martinez-Maure in [4] gave an algebraic equation of a non-circular constant width curve which is simpler than Rabinowitz's thanks to the notion of constant width hedgehogs. In particular, he used a parameterization of the constant width curve by a support function $p(t) = 8 - \sin(3\,t)$. However, in any case, it seems that the complexity of general algebraic equations is unavoidable for trigonometric polynomial support functions, because Bardet and Bayen showed in [1] that the minimum degree of an implicit equation defining a non-circular constant width curve of this kind is 8.

We propose a method for finding the algebraic equation based on the same technique used by Rabinowitz in [6] and by Martinez-Maure in [4] by the aid of Chebyshev polynomials. In addition, we provide an analogous method to obtain similar conclusions in the case of Zindler curves. The method is reduced to compute the resultant of two polynomials of degrees $2\,n + 2$ and $n + 1$ (Theorems 2.1 and 2.2), so that symbolic computation is usually needed to compute the algebraic equation.

1. Duality between curves of constant width and Zindler curves

A curve γ is said to be parameterized by a support function h if it can be written as

$$\gamma(t) = h(t)\,(\cos t,\, \sin t) + h'(t)\,(-\sin t,\, \cos t),$$

where h is 2π-periodic. The curve γ is called a hedgehog.

Definition 1 .1. A *h edgehog* parameterized by a support function h is *of constant width* d if

$$h(t) + h(t + \pi) = d.$$

A hedgehog γ is called *projective* if it is of zero constant width: $h(t) + h(t + \pi) = 0$.

In a hedgehog of constant width, the chord which measures the constant width can be proven to be orthogonal to the pair of tangent lines.

A common constraint for the definition of Zindler curves is that the halving chords cut the curve at precisely two points (and not more). Mampel in [3] considered generalized Zindler curves dropping this constraint.

Definition 1 .2. A regular closed curve α is called a *generalized Zindler curve* if there is a continuous motion of a constant length chord with its endpoints along α such that the length of α is split into two halves by these endpoints.

We will focus on generalized Zindler curves such that for each direction there is one and only one halving chord. These curves will be called *standard generalized Zindler curves.*

Hedgehogs of constant width can be related to standard generalized Zindler curves via offsets and front tracks. This give rise to the following duality [8]:

Theorem 1.3. *There is a one-to-one correspondence between hedgehogs of constant width and standard generalized Zindler curves.*

2. Algebraic equations for constant width curves and Zindler curves

Let γ be a projective hedgehog parameterized by a support function of the kind

$$p(t) = \frac{1}{b}\sin\big(n\,t\big), \tag{1}$$

where $b \in \mathbb{R}$ and $n = 2\,k + 1$, for $k \in \mathbb{N}$. The offset to γ at a distance a is a hedgehog of constant width $2\,a$ that can be parameterized as:

$$\alpha(t) = \big(a + p(t)\big)\,(\cos t, \sin t) + p'(t)\,(-\sin t, \cos t).$$

The front wheel track curve to γ at a distance d is a standard generalized Zindler curve for halving chords of length $2\,d$. It can be parameterized by

$$\beta(t) = p(t)\,(\cos t, \sin t) + \big(d + p'(t)\big)\,(-\sin t, \cos t).$$

The objective is to provide an explicit method to compute the algebraic equation of any of these curves α and β. The reader can find a detailed description in [7].

Recall that the Chebyshev polynomial of degree n, T_n, can be defined recursively as

$$\begin{aligned} T_0(x) &= 1,\\ T_1(x) &= x,\\ T_n(x) &= 2\,x\,T_{n-1}(x) - T_{n-2}(x), \quad n \geq 2. \end{aligned}$$

Define

$$p_{n-1}(x) = \sum_{k=0}^{\frac{n-1}{2}} \binom{n}{2\,k} (-1)^k\, x^{2k}\, (1 - x^2)^{\frac{n-2k-1}{2}}. \tag{2}$$

The method for computing the algebraic equations of these curves is reduced to the computation of a resultant, as stated in the following theorems.

Theorem 2.1. *The algebraic equation of the constant width curve α can be obtained by computing the resultant of the polynomials*

$$\left(1-s^2\right)\left(a\,b+(-1)^k\,T_n(s)-n\,s\,p_{n-1}(s)\right)^2-b^2\,x^2$$

and

$$s\left(a\,b+(-1)^k\,T_n(s)\right)+n\left(1-s^2\right)p_{n-1}(s)-b\,y,$$

which are of degrees $2\,n+2$ and $n+1$, respectively, and where p_{n-1} is the polynomial defined by (2).

Theorem 2.2. *The algebraic equation of the Zindler curve β can be obtained by computing the resultant of the polynomials*

$$\left(1-c^2\right)\left(-b\,d-n\,T_n(c)+(-1)^k\,c\,p_{n-1}(c)\right)^2-b^2\,x^2$$

and

$$c\left(b\,d+n\,T_n(c)\right)+(-1)^k\left(1-c^2\right)p_{n-1}(c)-b\,y,$$

which are of degrees $2\,n+2$ and $n+1$, respectively, and where p_{n-1} is the polynomial defined by (2).

These two results also hold in general for hedgehogs of constant width and standard generalized Zindler curves.

Finally, it can be observed that the polynomials we use to compute the resultant are very similar for pairs of "dual" curves (constant width curves and Zindler curves), as well as the resulting algebraic equations. This is particularly clear in some examples, like the one considered in [7].

References

[1] Magali Bardet and Térence Bayen, *On the degree of the polynomial defining a planar algebraic curves of constant width*, 2013, https://arxiv.org/abs/1312.4358.
[2] Javier Bracho, Luis Montejano, and Déborah Oliveros, *Carousels, Zindler curves and the floating body problem*, Period. Math. Hungar. **49** (2004), no. 2, 9–23.
[3] K. L. Mampel, *Über Zindlerkurven*, J. Reine Angew. Math. **234** (1969), 12–44.
[4] Yves Martinez-Maure, *Noncircular algebraic curves of constant width: an answer to Rabinowitz*, Canad. Math. Bull. **65** (2022), no. 3, 552–556.
[5] Horst Martini, Luis Montejano, and Déborah Oliveros, *Bodies of constant width*, Birkhäuser/Springer, Cham, 2019, An introduction to convex geometry with applications.
[6] Stanley Rabinowitz, *A polynomial curve of constant width*, Missouri J. Math. Sci. **9** (1997), no. 1, 23–27.
[7] David Rochera, *Algebraic equations for constant width curves and Zindler curves*, J. Symbolic Comput. **113** (2022), 139–147.
[8] David Rochera, *Offsets and front tire tracks to projective hedgehogs*, Comput. Aided Geom. Design **97** (2022), Paper No. 102135, 7 pp.
[9] Konrad Zindler, *Über konvexe Gebilde II*, Monatsh. Math. Phys. **31** (1921), 25–56.

BCAM - Basque Center for Applied Mathematics
Email address: drochera@bcamath.org