UNIVERSIDAD DE GRANADA

IMAG
INSTITUTO DE MATEMÁTICAS
Universidad de Granada

Proceedings of the XIX EACA

Encuentros de Álgebra Computacional y Aplicaciones

GRANADA, SPAIN

18-20 May, 2026

EDITORS

José Gómez-Torrecillas

Francisco Javier Lobillo

Gabriel Navarro

Víctor Sotomayor

XIX Encuentro de Álgebra Computacional y Aplicaciones

Scientific Committee

María Emilia Alonso
Marta Casanellas
Francisco J. Castro-Jiménez
Carlos D'Andrea
Ignacio García Marco
Philippe Gimenez
José Gómez-Torrecillas
Laureano González-Vega
Manuel Ladra
Jorge Martín Morales
Francisco José Monserrat Delpalillo
Luis Miguel Pardo Vasallo
Sonia Pérez Díaz
Ana Romero

Organizing Committee

Raquel Fuentes
José Gómez-Torrecillas
Francisco Javier Lobillo
Gabriel Navarro
Víctor Sotomayor

Supported by

Agencia Estatal de Investigación (RED2022-134220-T)
Instituto de Matemáticas (IMAG)
Departamento de Física y Matemáticas (UAH)

Conference held in Granada on 18-20 May, 2026

Published by Departamento de Álgebra, Universidad de Granada.

ISBN: 978-84-09-87277-0

Contents

Preface

It is a pleasure to welcome all participants, speakers, and readers to the book of abstracts of the XIX Meeting on Computational Algebra and Applications (EACA 2026). Since its inception in 1995 at the University of Cantabria, this series of meetings has fostered a tradition of excellence in algorithmic algebra. For this nineteenth edition, we gather at the Institute of Mathematics of the University of Granada (IMAG) from May 18th to 20th, 2026, to continue exploring the field's diverse applications and its rich scientific interactions.

The spirit of EACA 2026 is primarily focused on the support and promotion of young researchers. We are mindful that the vitality of our discipline depends on generational renewal. Therefore, this meeting has established itself as a forum designed for PhD students and early-career researchers to not only present their progress but also to build networks of collaboration with established figures in the field, thus ensuring an innovative future for computational algebra.

This edition holds a special significance for our community, as it marks the third time that EACA is held in Granada. The return to Granada highlights the University's enduring vocation to mathematics. This commitment to scientific development in Spain finds its perfect expression in the IMAG's environment, which provides a dedicated space for rigorous collaboration and the exchange of ideas.

The quality of this volume is the result of a high-level scientific program, consisting of 5 plenary lectures, 38 accepted contributions and 7 posters. We would like to express our gratitude to all contributors and, specially, to the invited speakers for joining us in this meeting: Emanuela de Negri (Università di Genova), Ignacio García-Marco (Universidad de La Laguna), Teresa Krick (Universidad de Buenos Aires), Joachim Rosenthal (Universität Zürich), Piotr Zwiernik (Universitat Pompeu Fabra).

The excellence of the works presented here was ensured by the diligent efforts of our Scientific Committee: María Emilia Alonso (UCM), Marta Casanellas (UPC), Francisco J. Castro-Jiménez (US), Carlos D'Andrea (UB), Ignacio García Marco (ULL), Philippe Gimenez (UVA), José Gómez-Torrecillas (UGR), Laureano González-Vega (UC), Manuel Ladra (USC), Jorge Martín Morales (UZ), Francisco José Monserrat Delpalillo (UPV), Luis Miguel Pardo Vasallo (UC), Sonia Pérez Díaz (UAH), and Ana Romero (UR).

The organization of this event is the result of the coordinated effort of several institutions. We wish to express our deepest gratitude to:

The University of Granada, and particularly its Department of Algebra, for its efficient administrative and institutional support.

The IMAG (Institute of Mathematics of the University of Granada), for its hospitality and for making its excellent facilities and staff available to us.

The Department of Physics and Mathematics of the University of Alcalá (UAH), for its constant logistical support, as well as its financial assistance.

The EACA Network (Thematic Network on Symbolic Computation, Computational Algebra, and Applications), which receives financial support from the Agencia Estatal de Investigación (AEI) through the grant RED2022-134220-T, a fundamental pillar for the realization of this meeting.

We hope that this book of abstracts serves as a source of inspiration and that the sessions in Granada prove to be scientifically stimulating for everyone.

THE ORGANIZING COMMITTEE

Granada, May 2026

List of participants

Poonee Afsharijoo	CY Cergy Paris University
María Emilia Alonso	Universidad Complutense de Madrid
Jesús Baena Gómez	Universidad de Sevilla
Luca Bastioni	University of South Florida
Marta Casanellas	Universitat Politècnica de Catalunya
Francisco Jesús Castro Jiménez	University of Seville and IMUS
Junyan Chu	Kyoto University
Melcion Ciudad Bosch	Universitat de les Illes Balears
Pilar Coscojuela Escanilla	EPITA
Carlos D'Andrea	Universitat de Barcelona
Miguel de los Ríos de Antonio	Universidad de Valladolid
Emanuela de Negri	Università di Genova
Danai Deligeorgaki	Universitat de Barcelona
Aram Dermenjian	Universidad de Sevilla
Claudia Fevola	CUNEF Universidad
Adrián Fidalgo Díaz	Universidad de Valladolid
Jesús Fernández	Universitat Politècnica de Catalunya
Raquel Fuentes	Universidad de Granada
Victoria García	BarcelonaTech, U. Politècnica de Catalunya
Ignacio García Marco	Universidad de La Laguna
Marina Garrote López	Universitat Pompeu Fabra
Philippe Gimenez	Universidad de Valladolid
José Gómez-Torrecillas	Universidad de Granada
Isaac González Rodríguez	Universidad de La Laguna
Laureano González-Vega	CUNEF Universidad
Belinda Hazel Cáceres Barrera	University of La Laguna
William Giovanni Hernández Yanes	Universidad de La Laguna
Pedro González Pérez	Universidad Complutense de Madrid
Joel Hurtado Moreno	Universitat Politècnica de Catalunya
Daniel Jaén Guedes	Universidad de La Laguna
Antonio Jiménez Pastor	Universidad Politécnica de Madrid
Shizuo Kaji	Kyoto University
Anargyros Katsampekis	University of Ioannina
Teresa Krick	Universidad de Buenos Aires
Manuel Ladra González	Universidad de Santiago de Compostela
Edwin León Cardenal	Universidad de Zaragoza
Javier Lobillo Olmedo	University of South Florida
Francisco Javier Lobillo	Universidad de Granada
Leo Margolis	Universidad Autónoma de Madrid
Helena Martín Cruz	Universidad de Jaén
Jorge Martín Morales	Universidad de Zaragoza
Pablo Mazón	CUNEF Universidad
Stefano Mereta	CUNEF Universidad
José Monserrat Delpalillo	Universidad Politècnica de València
María Eulalia Montoro López	Universidad de Barcelona
José Manuel Muñoz Fuentes	Universidad de Granada
Pablo Munarriz Senosiain	Universidad de La Rioja

Gabriel Navarro	Universidad de Granada
José Fabrizio Pineda Ramos	Universidad de La Laguna
Brais Ramos Pérez	Universidade de Santiago de Compostela
Tomás Recio	Universidad Antonio de Nebrija
Joachim Rosenthal	University of Zurich
Rosario Rubio	Universidad Antonio de Nebrija
Luis José Santana Sánchez	Universidad de La Laguna
Javier Sendra Arranz	CUNEF Universidad
Víctor Sotomayor	Universidad de Granada
Sonia L. Rueda	Universidad Politécnica de Madrid
Daniele Taufer	KU Leuven
Josué Tonelli-Cueto	CUNEF Universidad
Mª Pilar Vélez Melón	Universidad Antonio de Nebrija
Piotr Zwiernik	Universitat Pompeu Fabra

Plenary talks

Generalized binomial edge ideals are Cartwright-Sturmfels

A. Conca*, E. de Negri*◇, V. Welker†

◇ *Main speaker at EACA 2026*

* *Dipartimento di Matematica, Università di Genova*

† *Fachbereich Mathematik und Informatik, Philipps Universität Marburg*

aldo.conca@unige.it, emanuela.denegri@unige.it, welker@mathematik.uni-marburg.de

Abstract. Let X be an $m \times n$-matrix of indeterminates and let $G = ([n], E)$ be a graph. The generalized binomial edge ideal associated to G is the ideal I_G generated by the 2-minors of X obtained by choosing two arbitrary rows and two columns j, k such that $\{j, k\} \in E$. In earlier joint work with A. Conca and E. Gorla, it was shown that I_G is Cartwright-Sturmfels in the case $G = K_n$ and for arbitrary graphs G when $m = 2$. We prove that the Cartwright-Sturmfels property holds for all m and G, by establishing general results on ideal constructions that preserve this property. We also provide classes of examples and counterexamples for higher size minors.

Introduction

Ideals with a radical initial ideal are special: their homological relationship with the initial ideal is exceptionally tight. This intuition underlies Herzog's conjecture, now a theorem proved in [6], and it is precisely why such ideals are nowadays referred to as Herzog ideals.

A $\mathbb{Z}^n$-graded ideal in a $\mathbb{Z}^n$-graded polynomial ring is Cartwright-Sturmfels if its $\mathbb{Z}^n$-graded generic initial ideal is radical (this is one of the possible definitions). In fact, every initial ideal of a Cartwright-Sturmfels ideal is radical. Over the last years, several families of Cartwright-Sturmfels ideals have been identified [2–5, 7, 9], and the Hilbert-schemes associated to them have been investigated [11].

In this talk we show that generalized binomial edge ideals are also Cartwright-Sturmfels, see Theorem 7. We also give two auxiliary results concerning general Cartwright-Sturmfels ideals. Firstly, we describe certain Cartwright-Sturmfels subideals of a given Cartwright-Sturmfels ideal. Secondly, we show that the sum of two Cartwright-Sturmfels ideals is Cartwright-Sturmfels if the multidegrees of the generators of the two ideals overlap at most in one component. We conclude the talk with a discussion of families of higher-order minors that define Cartwright-Sturmfels ideals and families that do not define Cartwright-Sturmfels ideals.

J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, V. Sotomayor (eds.): Proceedings of the XIX EACA, pp. 13-16 (2026). ISBN: 978-84-09-87277-0

Cartwright-Sturmfels ideals

Let K be an infinite field and let $S = K[x_{ij} \mid 1 \leq j \leq n,\ 1 \leq i \leq m_j]$ be the polynomial ring over K endowed with the $\mathbb{Z}^n$-grading induced by setting $\deg(x_{ij}) = e_j$, where $e_j \in \mathbb{Z}^n$ is the j-th standard basis vector. Let $>$ be a term order on S.

For a $\mathbb{Z}^n$-graded S-module $M = \oplus_{a\in\mathbb{N}^n} M_a$ the $\mathbb{Z}^n$-graded Hilbert series of M is defined as the formal power series

$$\mathrm{HS}_M(Z_1, \ldots, Z_n) = \sum_{a\in\mathbb{N}^n} (\dim_K M_a) Z^a \in \mathbb{Q}[[Z_1, \ldots, Z_n]].$$

As in the standard $\mathbb{Z}$-graded situation, since K is infinite there exists a non-empty Zariski open $U \subseteq G$ such that $\mathrm{in}_>(gI) = \mathrm{in}_>(g'I)$ for all $g, g' \in U$, where $\mathrm{in}_>(I)$ is the initial ideal of I with respect to $>$. We call such a g a generic $\mathbb{Z}^n$-graded change of coordinates.

Definition 1. The $\mathbb{Z}^n$-graded generic initial ideal $\mathrm{gin}_>(I)$ of I with respect to $>$ is the ideal $\mathrm{in}_>(gI)$, where g is a generic $\mathbb{Z}^n$-graded coordinate change.

Let $B = B_{m_1}(K) \times \cdots \times B_{m_n}(K)$ be the Borel subgroup of G of upper triangular matrices in G. It turns out that $\mathrm{gin}(I)$ is fixed by the action of B. Ideals fixed by B are called Borel-fixed ideals.

We can now give the definition of Cartwright-Sturmfels ideals.

Definition 2. A $\mathbb{Z}^n$-graded ideal I of S is Cartwright-Sturmfels, or CS for short, if there exists a radical Borel-fixed monomial ideal which has the same $\mathbb{Z}^n$-graded Hilbert series as I.

To prove Theorem 7 we use some auxiliary results concerning general Cartwright-Sturmfels ideals, which are interesting on their own. First one is that the CS property is inherited by ideals generated by all elements of a fixed squarefree $\mathbb{Z}^n$-degree.

Lemma 3. *Let $I \subset S$ be a CS ideal and $A \subseteq [n]$. Let J be the ideal of S generated by the vector space I_A. Then J is CS and $\mathrm{in}_>(J)$ is generated by the monomial vector space $\mathrm{in}_>(I_A)$ for every term order $>$ of S.*

By using this lemma we give a criterion when the CS property is inherited by ideals which are generated by all polynomials from a set of squarefree $\mathbb{Z}^n$-degrees in a CS ideal.

Proposition 4. *Let $\mathcal{F} \subseteq 2^{[n]}$ such that:*

$$\text{if } A, B \in \mathcal{F} \text{ and } A \cap B \neq \emptyset \text{ then } A \cup B \in \mathcal{F}. \tag{1}$$

Let I be a CS ideal and let J be the ideal generated by the vector spaces I_A with $A \in \mathcal{F}$. Then J is CS. More precisely, for every term order $>$ the initial ideal $\mathrm{in}_>(J)$ is generated by the monomial vector spaces $\mathrm{in}_>(I_A)$ with $A \in \mathcal{F}$.

Note that for a $\mathbb{Z}^n$-ideal J generated in $\mathbb{Z}^n$ degrees $\leq e_1 + \ldots + e_\ell$ and a $\mathbb{Z}^n$-graded ideal H generated in degrees $\leq e_{\ell+1} + \cdots + e_n$ it is easy to see that if J and H are CS then so is $J + H$. Indeed we prove that a mild overlap of degrees still allows the same conclusion.

Proposition 5. *Let I and J be CS ideals such that for some $1 \leq \ell \leq n$ the ideal I is generated in degrees $\leq e_1 + \cdots + e_\ell$ and J is generated in degrees $\leq e_\ell + \cdots + e_n$. Then $I + J$ is CS.*

Binomial edges ideals

We now specialize to the situation when $S = K[X]$, with X a generic matrix of size $m \times n$ with the $\mathbb{Z}^n$-graded structure given by $\deg x_{ij} = e_j$ for every $j = 1, \ldots, n$. The ideal $I_2(X)$ generated by the 2-minors of X is known to be CS, see [1, Theorem 2.1].

In particular, by [2], for every $A \subseteq [n]$ the degree A component of the $\mathbb{Z}^n$-graded generic initial ideal of $I_2(X)$ is generated by the monomials

$$\prod_{j \in A} x_{i_j j} \tag{2}$$

such that

$$i_j \in [m] \text{ for every } j \in A \text{ and } \sum_{j \in A} i_j \leq m(|A| - 1). \tag{3}$$

In a next step we confine the generating set of the ideal to minors of columns of X selected from the edge set of a graph. More precisely, an (undirected simple) graph $G = ([n], E)$ is a pair of a vertex set $[n]$ and an edge set E consisting of 2-element subsets of $[n]$.

Definition 6. The generalized binomial edge ideal $I_G(m)$ is the sum of the ideals generated by the 2-minors of the columns j, k of X as $\{j, k\}$ varies in E.

Note that if $m = 2$ the ideal $I_G(2)$ is the (ordinary) binomial edge ideal, introduced by by Herzog and collaborators in [8] and, independently, by Ohtani in [10]. $I_G(2)$ is known to be CS by virtue of [3, 5].

Generalized binomial edge ideals were introduced by Rauh [12], who proved that $I_G(m)$ is radical for every m by showing that it has a square-free initial ideal.

For $A \subseteq [n]$ we write G_A for the graph (A, E_A) induced on A with edge set $E_A = \{e \in E \mid e \subseteq A\}$.

Main result of this talk is the following

Theorem 7. *Let $G = ([n], E)$ be a graph. Then the generalized binomial edge ideal $I_G(m)$ is CS for all m. More precisely, let $>$ be a term order satisfying*

$$x_{1j} > x_{2j} > \cdots > x_{mj} \text{ for every } j \in [n].$$

Then the $\mathbb{Z}^n$-graded generic initial ideal of $I_G(m)$ is generated by the monomials (2) *for the subsets $A \subseteq [n]$ such that G_A is connected and* (3) *is satisfied.*

References

[1] D. Cartwright, B. Sturmfels: The Hilbert scheme of the diagonal in a product of projective spaces. *Int. Math. Res. Not.* **9**, 1741–1771 (2010).

[2] A. Conca, E. De Negri, E. Gorla: Multigraded generic initial ideals of determinantal ideals. *Homological and computational methods in commutative algebra*, Springer INdAM Ser. **20**, 81–96 (2017).

[3] A. Conca, E. De Negri, E. Gorla: Cartwright-Sturmfels ideals associated to graphs and linear spaces. *J. Comb. Algebra* **2**(3), 231–257 (2018).

[4] A. Conca, E. De Negri, E. Gorla: Universal Gröbner bases and Cartwright-Sturmfels ideals. *Int. Math. Res. Not.* **7**, 1979–1991 (2020).

[5] A. Conca, E. De Negri, E. Gorla: Radical generic initial ideals. *Vietnam J. Math.* **50**(3), 807–827 (2022).

[6] A. Conca, M. Varbaro: Square-free Gröbner degenerations. *Invent. Math.* **221**, 713–730 (2020).

[7] A. Conca, V. Welker: Lovász-Saks-Schrijver ideals and coordinate sections of determinantal varieties. *Algebra Number Theory* **13**, 455–484 (2019).

[8] J. Herzog, T. Hibi, F. Hreinsdóttir, T. Kahle, J. Rauh: Binomial edge ideals and conditional independence statements. *Adv. in Appl. Math.* **45**, 317–333 (2010).

[9] M. Koji, T. Koichiro: Standard multigraded Hibi rings and Cartwright-Sturmfels ideals. *Preprint* (2025).

[10] M. Ohtani: Graphs and ideals generated by some 2-minors. *Comm. Algebra* **39**, 905–917 (2011).

[11] R. Ramkumar, A. Sammartano: Cartwright-Sturmfels Hilbert schemes. *Preprint* (2024).

[12] J. Rauh: Generalized binomial edge ideals. *Adv. in Appl. Math.* **50**, 409–414 (2013).

Computing invariants of Cayley graphs of groups

I. García-Marco
Instituto de Matemáticas y Aplicaciones de la ULL (IMAULL), Universidad de La Laguna
iggarcia@ull.edu.es

Abstract. In this talk we study Cayley graphs as a bridge between group theory and combinatorics, with an emphasis on computational aspects. We focus on two graph parameters that are hard to compute in general: the chromatic number and the genus. We present results illustrating how algebraic structure and symmetry can be exploited to analyze these invariants. Our approach combines theoretical methods with computer-assisted exploration.

Introduction

Cayley graphs of groups occupy a remarkable position at the interface of algebra, combinatorics, and geometry. They provide a natural way to encode the structure of a group into a graph: for a group G and a generating set $C \subseteq G$, the (undirected, right) *Cayley graph* $\mathrm{Cay}(G, C)$ has vertex set G and $a, b \in G$ are adjacent if $a^{-1}b \in C$. This correspondence makes Cayley graphs especially attractive objects of study, since combinatorial properties of the graph often reflect algebraic features of the underlying group.

From a computational perspective, this interaction is particularly valuable. Many graph invariants of central interest are notoriously difficult to determine in general. However, when the graph arises as a Cayley graph, the symmetry induced by the regular action of the group can be exploited to simplify both theoretical analysis and algorithmic computation. In this talk we will address problems related to two parameters of the graph: the chromatic number and the genus.

The new results that will be presented in this talk have been obtained in collaboration with Kolja Knauer; some are included in [5], while the rest are part of ongoing work.

The chromatic number of a group

In 1978, Babai [1] proved that every group admits a 3-colorable Cayley graph. More precisely, if we define $\chi_{\min}(G)$ as the minimum chromatic number among all Cayley graphs of G, then the following holds:

Theorem 1 (Babai)**.** *For a finite group G, one has:*

$$\chi_{\min}(G) = \begin{cases} 1 & \text{if } G \text{ is trivial,} \\ 2 & \text{if } G \text{ has a subgroup of index } 2, \\ 3 & \text{otherwise.} \end{cases}$$

J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, V. Sotomayor (eds.): Proceedings of the XIX EACA, pp. 17-21 (2026). ISBN: 978-84-09-87277-0

A Cayley graph is *minimal* if C is an inclusion-minimal generating set of G. In the same work, he raised the following question:

> «Does there exist a finite constant c such that every Cayley graph of a finite group with respect to a minimal generating set has chromatic number at most c?»

In 1994 [2], he conjectured a negative answer. Note that assuming minimality here is essential. The study of this problem motivates the definition of the *maximum chromatic number* of a finite group G, $\chi_{\max}(G)$, as the maximum chromatic number of $\mathrm{Cay}(G, C)$, where C ranges over all minimal generating sets of G.

A group is called *Dedekind* if all its subgroups are normal. Clearly, this includes all abelian groups and, by Dedekind's classification, very few others.

Theorem 2. *If G is a Dedekind group or a generalized dihedral group, then $\chi_{max}(G) \leq 3$.*

For the next result, we denote by $\Phi(G)$ the *Frattini subgroup* of G, that is, the intersection of all maximal proper subgroups of G, or $\Phi(G) = \{e\}$ if it has no maximal proper subgroups.

Lemma 3. *Let G be a group with Frattini subgroup $\Phi(G)$. Then:*

$$\chi_{\max}(G) \leq \chi_{\max}(G/\Phi(G)).$$

If a group G is nilpotent, then $G/\Phi(G)$ is abelian (and the converse also holds for finite groups). This fact, together with the previous lemma and Theorem 2 yield the following:

Corollary 4. *If G is a nilpotent group, then $\chi_{\max}(G) \leq 3$.*

We don't know if Babai's question has a positive answer even for solvable groups. The example in Figure 1 shows that there exist solvable groups with chromatic number 4. Combining our results, together with an exhaustive search using the datasets [3, 4] we verified that the chromatic number is at most 4 for all groups of order at most 512.

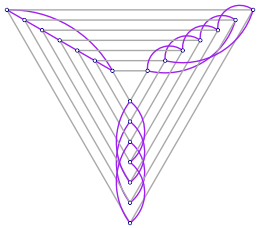


Figure 1. The graph $\mathrm{Cay}(\mathbb{Z}_3 \rtimes \mathbb{Z}_7, \{(0,1),(1,0)\})$ *has chromatic number* 4.

The genus of a group

An embedding of a graph X in a surface S is a representation of X on S in which the vertices are drawn as points and the edges as curves that intersect only at vertices.

A group G is planar if there exists a generating set C of G such that the graph $\mathrm{Cay}(G, C)$ is planar. A classical theorem of Maschke [7] characterizes the planar groups, namely: $\mathbb{Z}_n, D_n, A_4, S_4, A_5, \mathbb{Z}_2 \times \mathbb{Z}_n, \mathbb{Z}_2 \times D_n, \mathbb{Z}_2 \times A_4, \mathbb{Z}_2 \times S_4, \mathbb{Z}_2 \times A_5$.

For a nonplanar graph X, its *non-orientable genus* $\overline{\gamma}(X)$ is the minimum genus among all non-orientable surfaces into which the graph can be embedded. Likewise, for a group G, its non-orientable genus $\overline{\gamma}(G)$ is the minimum genus among all its (minimal) Cayley graphs with respect to a generating set.

We define:

$$\begin{array}{rcl} f(k) & := & \#\{G \text{ group } \mid \overline{\gamma}(G) = k\}, \\ g(k) & := & \#\{X \text{ minimal Cayley graph } \mid \overline{\gamma}(X) = k\}; \end{array}$$

by definition, we have that $f(k) \leq g(k)$.

By results of Proulx and Tucker (see [6] for a book exposition), for every surface S with $\chi(S) < 0$ there are only finitely many minimal Cayley graphs embeddable on S that are not embeddable into sphere or torus. Further note that the torus can be embedded into the Dyck surface. Hence, for every $k > 3$ the values $f(k)$ and $g(k)$ are finite.

It was claimed in [6, Theorem 6.4.4] that $f(1) = g(1) = 1$. Years later, in 2009, Tucker mentions in [11] that J. Hannon (one of his students) had found that $S_3 \times \mathbb{Z}_3$ is another non-planar group that can be embedded in the projective plane and, consequently, $f(1) \geq 2$. We prove the following:

Theorem 5. *There are precisely three minimal Cayley graphs of non-orientable genus* 1*, each being the Cayley graph of exactly one group, which are* $\mathbb{Z}_3 \times \mathbb{Z}_3$*,* $S_3 \times \mathbb{Z}_3$*, and* A_5*. Hence,* $f(1) = 2$ *and* $g(1) = 3$ *(see Figure 2).*

In the same paper, it is suggested that there might be no groups of non-orientable genus 2 and 4. There are some infinite families of large genus known [8, 9]. Furthermore it is known that $\overline{\gamma}(S_5) = 5$ [10] and hence $f(5) \geq 1$.

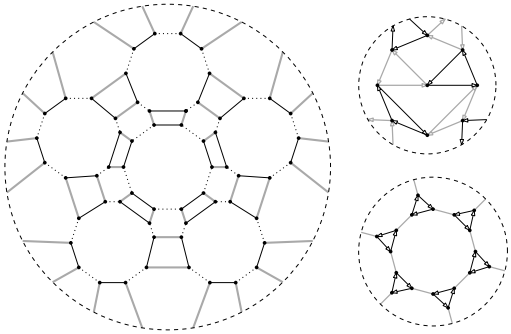


Figure 2. Embeddings in the projective plane of $\mathrm{Cay}(A_5, \{(1,2)(4,5), (1,3)(4,5), (1,4)(3,5)\})$*,* $\mathrm{Cay}(\mathbb{Z}_3 \times \mathbb{Z}_3, \{(0,1), (1,0)\})$*, and* $\mathrm{Cay}(\mathbb{Z}_3 \times S_3, \{(0,(12)), (1,(123))\})$*.*

Theorem 6. *Let $n \geq 2$. Then the dicyclic group*

$$\mathrm{Dic}_n = \left\langle a, b \mid a^{2n} = e,\ b^2 = a^n,\ b^{-1}ab = a^{-1} \right\rangle,$$

of order $4n$ has non-orientable genus 2 (see Figure 3).

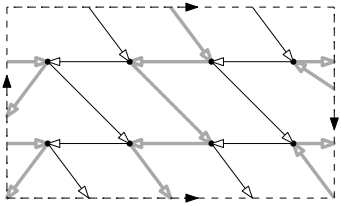


Figure 3. An embedding of $\mathrm{Cay}(Q_8, \{a, b\})$ *in the Klein bottle.*

Theorem 7. *Let $p > 3$ be a prime. The group $\mathbb{Z}_p \times \mathbb{Z}_p$ has non-orientable genus 3.*

The following table summarizes the known values of $f(k)$ and $g(k)$:

	projective plane $k = 1$	Klein bottle $k = 2$	Dyck surface $k = 3$	$k > 3$
$f(k)$	2	∞	∞	$< \infty$
$g(k)$	3	∞	∞	$< \infty$

References

[1] L. Babai: Chromatic number and subgraphs of Cayley graphs. *Theor. Appl. Graphs, Proc. Kalamazoo 1976, Lect. Notes Math.* **642**, 10–22 (1978).

[2] L. Babai: Automorphism groups, isomorphism, reconstruction. *Handbook of combinatorics*, Vol. 1-2, pages 1447–1540. Amsterdam: Elsevier (North-Holland); Cambridge, MA: MIT Press (1995).

[3] R.J. Evans, K. Knauer, P. Potocnik: Minimal Cayley graphs on 2 to 511 vertices (excluding 384) (Version 0.1) [Data set]. *Zenodo* (2025).

[4] R.J. Evans, K. Knauer, P. Potocnik: Minimal Cayley graphs on 384 vertices [Data set]. *Zenodo* (2025).

[5] I. García-Marco, K. Knauer: Coloring minimal Cayley graphs. *Eur. J. Combin.* **125**, 104108 (2025).

[6] J.L. Gross, T.W. Tucker: Topological graph theory. Mineola, NY: Dover Publications, preprint of the 1987 orig. edition (2001).

[7] H. Maschke: The representation of finite groups, especially of the rotation groups of the regular bodies of three-and four-dimensional space, by Cayley's color diagrams. *Amer. J. Math.* **18**(2), 156–194 (1896).

[8] T. Pisanski, A. White: Nonorientable embeddings of groups. *Eur. J. Comb.* **9**(5), 445–461 (1988).

[9] T. Pisanski, T.W. Tucker, D. Witte: The non-orientable genus of some metacyclic groups. *Combinatorica* **12**(1), 77–87 (1992).

[10] V.K. Proulx: On the genus of symmetric groups. *Trans. Am. Math. Soc.* **266**, 531–538 (1981).

[11] T.W. Tucker: The genus of a group. *Topics in topological graph theory*, 225–244. Cambridge University Press (2009).

Effective bounds for polynomial systems defined over the rationals

T. Krick
University of Buenos Aires and Conicet
krick@dm.uba.ar

Abstract. Given computer algebra problems defined by polynomials with rational coefficients, I will present tools that help measuring their complexity by providing bounds on the degrees and heights (i.e., bit-sizes) of the output in terms of those of the input. I will focus on the case where the input polynomials have a finite number of solutions in $\mathbb{C}^n$, discussing an arithmetic Nullstellensatz in the case of no solutions and an arithmetic Bézout inequality. I will also present several examples and applications.

A non-zero polynomial $f = \sum_{\alpha\in\mathbb{N}^n} c_\alpha \boldsymbol{x}^\alpha \in \mathbb{Z}[\boldsymbol{x}] = \mathbb{Z}[x_1,\dots,x_n]$, where $\mathbb{Z}$ is the ring of integer numbers, has naturally three parameters that measure its complexity: its number of variables n, its degree $\deg(f) := \max\{|\alpha| = \alpha_1+\cdots+\alpha_n \text{ for } \alpha = (\alpha_1,\dots,\alpha_n) \text{ such that } c_\alpha \neq 0\}$, and its (binary logarithmic) height

$$\mathsf{h}(f) := \max_\alpha\{\log_2|c_\alpha| : c_\alpha \neq 0\},$$

which basically represents the number of bits needed to write any of its coefficients. We note that the maximum number of coefficients of such a polynomial of degree d in n variables equals $\binom{d+n}{n} \approx d^n$, so that its input size, if it has height h and we want to describe all its coefficients, is of order $d^n h$, exponential in the number of variables n.

Given polynomials $f_1,\dots,f_s \in \mathbb{C}[\boldsymbol{x}]$ the (affine) algebraic variety

$$V := V_{\mathbb{C}}(f_1,\dots,f_s) = \{\boldsymbol{\zeta}\in\mathbb{C}^n : f_1(\boldsymbol{\zeta}) = \cdots = f_s(\boldsymbol{\zeta}) = 0\} \subset \mathbb{C}^n$$

is the set of common (complex) roots of these polynomials. When $f_1,\dots,f_s \in \mathbb{C}[\boldsymbol{x}]$, the *Nullstellensatz*, a cornerstone of Algebraic Geometry proved by Hilbert in 1893, establishes that $V = \emptyset$ if and only if there exist $g_1,\dots,g_s \in \mathbb{C}[\boldsymbol{x}]$ such that a Bézout identity

$$1 = g_1 f_1 + \cdots + g_s f_s$$

holds. Since this is a non-constructive statement, the *effective* Nullstellensatz deals with showing a priori degrees for existing coefficients polynomials $g_1,\dots,g_s$ in this case in terms of the degrees of the input polynomials $f_1,\dots,f_s$. The best degree bound, obtained by Jelonek in 2005, after previous work by Hermann, Brownawell, Caniglia-Galligo-Heintz, Kollár and Sombra, states in particular that when $\max_i \deg(f_i) = d$ and $s \leq n+1$, there exist such $g_1,\dots,g_s$ with $\deg(g_i)+\deg(f_i) \leq d^s$, and this bound is optimal for $s = n$.

J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, V. Sotomayor (eds.): Proceedings of the XIX EACA, pp. 22-23 (2026).
ISBN: 978-84-09-87277-0

When the input polynomials have integer coefficients, i.e. $f_1, \ldots, f_s \in \mathbb{Z}[\boldsymbol{x}]$, the Nullstellensatz reads as

$$V = \emptyset \iff \exists\, a \in \mathbb{Z} \setminus \{0\} \text{ and } g_1, \ldots, g_s \in \mathbb{Z}[\boldsymbol{x}] \text{ s.t. } a = g_1 f_1 + \cdots + g_s f_s.$$

The *arithmetic* Nullstellensatz deals with providing a height bound for a and simultaneous degrees and heights bounds for the polynomials $g_1, \ldots, g_s$: that is one of the questions I will address in this talk.

When $f_1, \ldots, f_s \in \mathbb{C}[\boldsymbol{x}]$ define a finite non-empty variety V of cardinality $D \geq 1$, the *Bézout inequality*, a nowadays crucial tool in Computational Algebra, states that for $d := \max_i \deg(f_i)$ we have $D \leq d^n$. I will discuss arithmetic aspects of this Bézout inequality when the input polynomials $f_1, \ldots, f_s$ have integer coefficients. These in particular yield upper and lower bounds for the modules of all non-zero components of the common roots $\boldsymbol{\zeta} \in V$, upper and lower bounds for the separation between these roots. They also allow to derive upper height bounds for univariate polynomials parameterizing these finite common roots, and for a "remainder" of any integer polynomial p when dividing by $f_1, \ldots, f_s$.

All the results I will present are included in the survey article *Effective bounds for polynomial systems over the rationals*, `https://arxiv.org/pdf/2506.18144`, to appear in the Special Issue RTCA2023 at Springer collection TMSC, and the references mentioned therein.

Computer algebra challenges related to post-quantum cryptography

J. Rosenthal
Institute of Mathematics, University of Zurich
rosenthal@math.uzh.ch

Abstract. Currently there is an ongoing standardization process for new cryptographic systems which are presumably quantum computer safe. In this talk we survey this process and we explain several computer algebra problems directly linked to some of the proposed systems.

Public-key cryptography lies at the heart of modern digital security, underpinning key exchange, digital signatures, and secure internet communications. For decades, the security of these widely deployed systems has relied almost entirely on the hardness of integer factorization and the discrete logarithm problem over elliptic curves. However, the anticipated advent of cryptographically relevant quantum computers threatens to render these traditional systems obsolete.

In response, the cryptographic community has pivoted toward post-quantum cryptography (PQC)–systems designed to remain secure against both classical and quantum cryptanalysis. A primary driver of this global transition is the ongoing National Institute of Standards and Technology (NIST) PQC standardization process. This rigorous, multi-year effort to evaluate and standardize quantum-resistant public-key cryptographic algorithms has already resulted in the selection of the first primary standards, while continuing to evaluate promising alternative architectures.

The security of these newly proposed and standardized schemes rests on fundamentally different mathematical foundations, shifting the focus toward challenging algorithmic problems in algebra, geometry, and coding theory. This lecture will provide a comprehensive overview of the currently evaluated PQC systems and the trajectory of the NIST standardization process.

In this context, we will delve into the critical intersection between computer algebra and post-quantum security by describing several specific algebraic challenges whose computational complexity is directly linked to the robustness of these new systems. Highlights will include the Lattice Isomorphism Problem (LIP) –the computational challenge of determining whether two given lattices are orthogonally equivalent– and the Code Equivalence Problem, a foundational hurdle in code-based cryptography that assesses whether two linear codes are equivalent under coordinate permutation and scaling. By analyzing these and other com-

J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, V. Sotomayor (eds.): Proceedings of the XIX EACA, pp. 24-25 (2026).
ISBN: 978-84-09-87277-0

puter algebra challenges, this talk will illustrate the ongoing mathematical effort required to secure the next generation of cryptographic infrastructure.

Acknowledgements. Research supported by Swiss National Science Foundation, Armasuisse and Innosuisse.

References

[BBPS23] A. Barenghi, J.-F. Biasse, E. Persichetti, P. Santini: On the computational hardness of the code equivalence problem in cryptography. *Adv. Math. Commun.* **17**(1), 23–55 (2023).

[BMvT78] E.R. Berlekamp, R.J. McEliece, H.C.A. van Tilborg: On the inherent intractability of certain coding problems. *IEEE Trans. Inform. Theory* **24**(3), 384–386 (1978).

[CJL+16] L. Chen, S. Jordan, Y.K. Liu, D. Moody, R. Peralta, R. Perlner, D. Smith-Tone: Report on Post-Quantum Cryptography. Technical report NISTIR 8105, National Institute of Standards and Technology, April 2016.

[DvW22] L. Ducas, W. van Woerden: On the lattice isomorphism problem, quadratic forms, remarkable lattices, and cryptography. *Advances in Cryptology — EUROCRYPT*, Part III, volume 13277 of *Lecture Notes in Comput. Sci.*, 643–673, Springer (2022).

[Jou23] A. Joux: MPC in the head for isomorphisms and group actions. *Cryptology ePrint Archive*, Paper 2023/664 (2023).

[MMR07] G. Maze, C. Monico, J. Rosenthal: Public key cryptography based on semigroup actions. *Adv. Math. Commun.* **1**(4), 489–507 (2007).

[McE78] R.J. McEliece: A public-key cryptosystem based on algebraic coding theory. Technical report, DSN Progress Report, Jet Propulsion Laboratory, Pasadena (1978).

[ALR25] S.A. Otero, J.A. López Ramos: Cryptanalysis of a key exchange protocol based on a congruence-simple semiring action. *J. Algebra Appl.* **24**(9), 2550229 (2025).

[RoSc26] J. Rosenthal, S. Sconza: Semigroup action problems and their uses in post-quantum cryptography. *Cryptology ePrint Archive*, Paper 2026/462 (2026).

[NIS15] Committee on National Security Systems: Use of public standards for the secure sharing of information among national security systems. CNSS Advisory Memorandum (2015).

[WGR22] V. Weger, N. Gassner, J. Rosenthal: A survey on code-based cryptography. *ArXiv:2201.07119* (2022).

Tensor eigenvectors and identifiability: From spectral theory to Independent Component Analysis

P. Zwiernik*

Universitat Pompeu Fabra

* *The talk is based on joint work with Geert Mesters, Álvaro Ribot, and Anna Seigal.*

piotr.zwiernik@upf.edu

Abstract. The spectral theorem gives a complete description of real symmetric matrices: every such matrix admits an orthogonal basis of eigenvectors, and if the eigenvalues are distinct this basis is unique up to signs and permutations. For higher-order symmetric tensors, the situation is different: a tensor may have many eigenvectors but need not admit an orthogonal eigenbasis.

We study symmetric tensors that do admit such a basis. The basic idea is to encode an orthogonal eigenbasis by zero restrictions in a suitable coordinate system. The uniqueness question then becomes an algebraic identifiability problem: can two essentially different orthogonal bases give the same type of zero pattern? For a natural class of tensors, we show that the answer is generically no: the only remaining ambiguities are signs and permutations.

We also explain how the same algebraic structure appears in Independent Component Analysis. Classical ICA uses probabilistic independence, which makes higher-order cumulant tensors diagonal. Weaker conditions, such as mean independence, impose only selected zero restrictions on cumulant tensors, but these restrictions can still give generic identifiability.

Introduction

The spectral theorem for symmetric matrices says that every real symmetric matrix admits an orthogonal basis of eigenvectors. If the eigenvalues are distinct, this basis is uniquely determined up to signs and permutations. We ask to what extent this picture extends to higher-order tensors.

Let $S^r(\mathbb{R}^d)$ be the space of real symmetric tensors of order $r \geq 3$. A tensor $T \in S^r(\mathbb{R}^d)$ defines a homogeneous polynomial

$$f_T(x) = T(x, \ldots, x) = \sum_{i_1,\ldots,i_r=1}^{d} T_{i_1\cdots i_r} x_{i_1} \cdots x_{i_r}.$$

A unit vector $u \in \mathbb{R}^d$ is an eigenvector of T if

$$T(u, \ldots, u, \cdot) = \lambda u$$

J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, V. Sotomayor (eds.): Proceedings of the XIX EACA, pp. 26-29 (2026).
ISBN: 978-84-09-87277-0

for some $\lambda \in \mathbb{R}$. Equivalently, eigenvectors are the critical points of f_T on the unit sphere, or the critical points of

$$\min_{\lambda,u} \|T - \lambda u^{\otimes r}\|^2, \qquad \|u\| = 1.$$

Unlike in the matrix case, eigenvectors of a tensor do not usually form an orthogonal basis. The basic problem is: when does a tensor $T \in S^r(\mathbb{R}^d)$ admit an orthogonal basis of eigenvectors, and when is this basis uniquely determined?

We study this through zero restrictions. An orthogonal eigenbasis can be viewed as a coordinate system in which the tensor has a special sparse form. Uniqueness of the eigenbasis is then an identifiability question.

Zero restrictions and generic uniqueness

Consider the linear subspace

$$\mathcal{V} = \{T \in S^r(\mathbb{R}^d) : T_{ij\cdots j} = 0 \text{ for all } i \neq j\}.$$

Equivalently, $T(e_j, \ldots, e_j, e_i) = 0$ for all $i \neq j$. Hence $T(e_j, \ldots, e_j, \cdot)$ has no component in any direction e_i with $i \neq j$, and so

$$T(e_j, \ldots, e_j, \cdot) = T_{j\cdots j} e_j.$$

Thus every tensor in $\mathcal{V}$ admits the standard orthonormal basis as an eigenbasis.

The orthogonal group $\mathsf{O}(d)$ acts on $S^r(\mathbb{R}^d)$ by

$$(Q \bullet T)_{i_1 \cdots i_r} = \sum_{j_1,\ldots,j_r=1}^{d} Q_{i_1 j_1} \cdots Q_{i_r j_r} T_{j_1 \cdots j_r}, \qquad f_{Q\bullet T}(x) = f_T(Q^\top x).$$

If $S \in \mathcal{V}$ and $T = Q \bullet S$, then the columns of Q form an orthonormal eigenbasis of T. Thus $Q \bullet \mathcal{V}$ is the class of tensors whose distinguished eigenbasis is given by the columns of Q.

The uniqueness question is whether a tensor can lie in two such classes, $Q \bullet \mathcal{V}$ and $Q' \bullet \mathcal{V}$, for essentially different orthogonal matrices Q and Q'. Equivalently, after choosing coordinates so that $T \in \mathcal{V}$, we ask which orthogonal changes of coordinates keep T in $\mathcal{V}$:

$$\mathcal{G}_T(\mathcal{V}) = \{Q \in \mathsf{O}(d) : Q \bullet T \in \mathcal{V}\}.$$

Here $Q \bullet T \in \mathcal{V}$ means that the rows of Q form another orthonormal eigenbasis of the original tensor T.

Theorem 1. *Let $r \geq 3$ and $d \geq 2$. For a generic tensor $T \in \mathcal{V}$, the set $\mathcal{G}_T(\mathcal{V})$ consists exactly of signed permutation matrices.*

Thus, generically, the orthogonal eigenbasis encoded by the zero restrictions is unique up to signs and permutations. The proof combines algebraic geometry with the tensor eigenvector equations: the condition $Q \bullet T \in \mathcal{V}$ forces the rows of Q to be eigenvectors of T, and one shows that generically no orthonormal eigenbasis other than the coordinate basis satisfies the same zero restrictions.

Connection to Independent Component Analysis

The same algebraic structure appears in Independent Component Analysis (ICA), a classical problem in signal processing and statistics. In ICA, one observes linear mixtures of latent signals and tries to recover the original sources. A standard example is blind source separation, where several microphones record different mixtures of the same underlying voices or instruments.

Suppose that an observed random vector $Y = (Y_1, \dots, Y_d)$ satisfies

$$AY = X,$$

where A is an unknown invertible unmixing matrix and X is a vector of hidden sources. Classical ICA assumes that the components of X are probabilistically independent. To relate this to tensors, recall that the moment generating function of X is

$$M_X(t) = \mathbb{E}\exp(t^\top X).$$

When M_X is finite in a neighbourhood of the origin, it determines the distribution of X. It is often more convenient to work with the cumulant generating function $K_X(t) = \log M_X(t)$. The order-r cumulant tensor $\kappa_r(X)$ is the symmetric tensor in $S^r(\mathbb{R}^d)$ obtained from the derivatives

$$(\kappa_r(X))_{i_1\cdots i_r} = \left.\frac{\partial^r K_X(t)}{\partial t_{i_1}\cdots\partial t_{i_r}}\right|_{t=0}.$$

Independence of the components of X is equivalent, under this mild analytic assumption, to the additivity $K_X(t) = \sum_i K_{X_i}(t_i)$. Equivalently, all mixed cumulants vanish; in tensor language, all cumulant tensors $\kappa_r(X)$ are diagonal. Cumulants transform multilinearly under linear changes of coordinates, so

$$\kappa_r(X) = A \bullet \kappa_r(Y).$$

ICA can therefore be viewed as the problem of finding a change of coordinates that puts observed cumulant tensors into a structured form. Under full independence this form is diagonal. This tensor point of view is classical in ICA and signal processing. For accessible entry points, see Comon's original paper on ICA [1], his survey on tensor decompositions in signal processing [2], and the tensor references [3–5].

The point here is that full independence is not the only condition giving useful structure. In many applications, sources may fail to be independent but still satisfy weaker conditional moment restrictions. For instance, two signals may share a common volatility or scale factor. Their magnitudes may then be dependent through this shared random environment, even if selected conditional means remain zero. Such dependence is not captured by full independence, but it can still leave useful algebraic traces in higher-order moments.

This motivates assumptions such as mean independence. They do not imply that all mixed cumulants vanish, and hence they do not make the cumulant tensor diagonal. Instead, they imply only selected moment or cumulant restrictions. For instance, restrictions of the form

$$\mathbb{E}[X_i X_j^{r-1}] = 0 \qquad (i \neq j)$$

lead to vanishing entries $T_{ij\cdots j} = 0$. Thus the source cumulant tensor need not be diagonal, but it may lie in a space such as $\mathcal{V}$.

The theorem above shows that these fewer zero restrictions can still be rigid enough to identify the relevant coordinate system, generically up to signed permutations. This gives an algebraic explanation for identifiability beyond classical ICA.

Discussion

The results illustrate a general principle: statistical identifiability can often be reformulated as an algebraic problem about group actions and structured tensor spaces. Tensor spectral theory then gives a natural language for studying when a model is identifiable and what ambiguities remain.

Several concrete questions remain open. One is to describe the exceptional nongeneric tensors for which additional orthogonal eigenbases exist. Another is to give explicit equations and dimension formulas for the varieties of tensors with an orthogonal eigenbasis. More generally, one can ask which zero patterns, beyond the space $\mathcal{V}$ considered here, still give generic uniqueness. Related questions arise for non-symmetric tensors and for CP and Tucker decompositions.

For readers interested in the statistical side, [1] remains a standard entry point to ICA, while [6] studies identifiability beyond classical independence assumptions. For readers interested in tensor eigenvalues and algebraic geometry, [3–5, 7, 8] give useful complementary perspectives.

References

[1] P. Comon: Independent component analysis, a new concept? *Signal Process.* **36**(3), 287–314 (1994).

[2] P. Comon: *Tensor decompositions.* Mathematics in Signal Processing V, J.G. McWhirter and I.K. Proudler (eds.), pages 1–24. Clarendon Press, Oxford (2002).

[3] P. Comon, G. Golub, L.H. Lim, B. Mourrain: Symmetric tensors and symmetric tensor rank. *SIAM J. Matrix Anal. Appl.* **30**(3), 1254–1279 (2008).

[4] L.H. Lim: Singular values and eigenvalues of tensors: a variational approach. *Proceedings of the IEEE International Workshop on Computational Advances in Multi-Sensor Adaptive Processing (CAMSAP 2005)*, pages 129–132. IEEE (2005).

[5] L. Qi: Eigenvalues of a real supersymmetric tensor. *J. Symbolic Comput.* **40**(6), 1302–1324 (2005).

[6] G. Mesters, P. Zwiernik: Non-independent component analysis. *Ann. Statist.* **52**(6), 2506–2528 (2024).

[7] A. Ribot, A. Seigal, P. Zwiernik: Orthogonal eigenvectors and singular vectors of tensors. *ArXiv:2506.19009* (2025).

[8] A. Ribot, A. Seigal, P. Zwiernik: Beyond independent component analysis: identifiability and algorithms. *ArXiv:2510.07525* (2025).

Contributed talks

Tropical KP Theory on banana curves

S. Abenda*, T.Ö. Çelik†, C. Fevola◇‡, Y. Mandelshtam≀

◇ *Speaker at EACA 2026*

* *Università di Bologna and INFN*

† *MPI of Molecular Cell Biology and Genetics & Center for Systems Biology Dresden*

‡ *Department of Mathematics, CUNEF Universidad*

≀ *University of Michigan*

simonetta.abenda@unibo.it, celik@mpi-cbg.de, claudia.fevola@cunef.edu, yelenam@umich.edu

Abstract. The Kadomtsev–Petviashvili (KP) equation is the cornerstone of integrable systems; its solutions reflect deep connections in algebraic geometry. Banana curves are reducible rational curves obtained as a degeneration of hyperelliptic curves. In this work, we relate the family of KP multi-solitons arising from banana curves together with non-special divisors of fixed degree to the combinatorics of the tropical theta divisor of the curve. We describe the Voronoi and Delaunay polytopes and show that the latter are combinatorially equivalent to uniform matroid polytopes. As a consequence, the combinatorics of the tropical theta divisor canonically encodes the matroid and Grassmannian structures underlying the associated KP multi-soliton solutions. We define the Hirota variety of a banana graph, which parametrizes all tau functions arising from such a graph. Starting from the matroid arising from Delaunay polytopes and the periods in the tropical limit, we construct an explicit parametrization of this variety. This parametrization realizes the associated τ-function as a KP multi-soliton. Our framework specializes naturally to real and positive settings.

Introduction

This extended abstract summarizes the results of the paper [2], where full proofs and additional results can be found. The Kadomtsev–Petviashvili (KP) equation is a nonlinear partial differential equation

$$(-4u_t + 6uu_x + u_{xxx})_x = -3u_{yy}, \tag{1}$$

for an unknown function $u(x, y, t)$ of two spatial variables x, y and one time variable t, where subscripts denote partial derivatives. When the variables x, y, t are real, the form of (1) is the KP II equation. In what follows, for simplicity, we refer to (1) as the KP equation both in the real and complex settings. This prominent integrable equation models the propagation of long, weakly two-dimensional shallow water waves with slow variation along the transverse y-direction. The KP equation is among the most fundamental examples in the theory of integrable systems. It serves as an example of an integrable hierarchy whose solutions have dual geometric realizations through algebraic curves on one side and Grassmannians on the

J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, V. Sotomayor (eds.): Proceedings of the XIX EACA, pp. 31-35 (2026). ISBN: 978-84-09-87277-0

other. Understanding how these two realizations are related has been a central problem in the modern theory of integrable systems.

Two distinguished families of solutions are the finite-gap and the multi-soliton solutions. Finite-gap solutions are parametrized by algebraic curves, namely the spectral curves of the Lax operator, and are expressed in terms of Riemann theta functions. KP solitons admit a representation via Wronskian determinants and are parameterized by points in finite-dimensional Grassmannians. The relation between these classes has been deeply studied in recent years, see e.g., [3]. An alternative viewpoint on this correspondence comes from tropical geometry. In the tropical limit, the Riemann theta function becomes a finite sum of exponentials supported on the vertices of a polytope, called Delaunay polytope, see [4]. In this framework, soliton solutions appear as rational degenerations of finite-gap solutions, with their combinatorial structure encoded by tropical curves and their Jacobians.

In [2], we explore this correspondence for tropical degenerations associated with banana graphs, i.e., metric graphs with two vertices connected by $g+1$ edges, which naturally arise as tropical limits of hyperelliptic curves of genus g. We describe their tropical Jacobians and Voronoi–Delaunay decomposition, and establish their connections with matroid base polytopes, such as hypersimplices. A key aspect of our construction is the realization of the tropical Jacobian of the banana graph in a higher-dimensional space, where it appears as a projection of the $(g+1)$-dimensional hypercube. This representation plays a central role in relating the combinatorial structure of the tropical Jacobian to Grassmannians and soliton τ-functions. Our results thus provide a concrete geometric realization of the correspondence between tropical degenerations of algebraic curves and KP solitons, making explicit how tropical Jacobians and combinatorial polytopes capture the algebraic structure of integrable hierarchies.

The framework developed in [2] is the first step in a broader project aimed at understanding KP solitons arising from arbitrary metric graphs. It should be viewed as a detailed case study that foreshadows a much more general theory. Its full development is part of ongoing joint work by the authors. The case of banana graphs is treated in full detail not only because it is already rich enough to exhibit several key phenomena, but also because it provides an informative model illustrating the methods that will be used in greater generality.

Voronoi–Delaunay combinatorics of banana graphs

Let $\Gamma_g = (V, E)$ be the banana metric graph with two vertices v_1, v_2 connected by $n = g+1$ edges $e_1, \dots, e_n$, representing the branch points of a hyperelliptic curve of genus g. Figure 1 illustrates the graph Γ_g. The main results of [2] describe the combinatorial and geometric structure underlying KP multi-solitons arising from tropical degenerations associated with banana graphs. We give an explicit description of the Voronoi polytope of the tropical Jacobian of a banana graph, including its set of vertices and f-vector ([2, Theorem 3.1]), and show that the associated Delaunay polytopes are matroid polytopes. We resume this result in the following

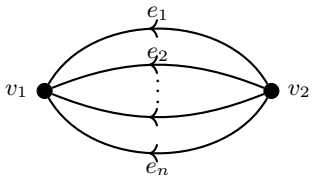


Figure 1. The banana graph of genus g with orientation ι_0.

Theorem 1. *For banana graphs of genus g, the associated Delaunay polytopes are combinatorially equivalent to hypersimplices $\Delta(k, n)$, and hence to matroid base polytopes of uniform matroids.*

More formally, this is the content of [2, Theorem 3.5] and [2, Corollary 3.6]). Furthermore, we identify the face poset of the Voronoi polytope with the poset of strongly connected orientations of the graph (see [5, Theorem 1]), and provide an explicit description of this correspondence in the case of banana graphs. As a consequence, each Voronoi vertex, together with a choice of graph vertex, canonically determines a matroid whose bases are in bijection with the corresponding Delaunay set, thereby linking the tropical Jacobian to the Grassmannian framework underlying KP solitons ([2, Theorem 3.12]).

To make the construction more explicit, recall that the vertices of the Voronoi polytope V_Q split into equivalence classes

$$V_Q = \bigsqcup_{k=1}^{g} [\mathbf{k}],$$

where $[\mathbf{k}]$ denotes the class of Voronoi vertices whose associated Delaunay polytope is combinatorially equivalent to the hypersimplex $\Delta_{k,n}$, with $n = g + 1$. A key point of the construction is that the Voronoi polytope of the banana graph is the projection of the cube $[-\frac{1}{2}, \frac{1}{2}]^n$ onto the hyperplane $\sum_i x_i = 0$. Hence each Voronoi vertex $\mathbf{a}$ comes from a cube vertex and determines a sign vector $\sigma(B^T\mathbf{a}) \in \{\pm 1\}^n$. This sign vector defines a strongly connected orientation ι_a by orienting e_i according to the sign of $(B^T\mathbf{a})_i$. When $\mathbf{a}$ belongs to the class $[\mathbf{k}]$, the corresponding Delaunay polytope $D_{\mathbf{a},Q}$ becomes, after translation by an explicit vector $s_{\mathbf{a}}$, the hypersimplex $\Delta_{k,n}$. Therefore the Delaunay points are naturally indexed by the bases of the uniform matroid $U_{k,n}$, and these same combinatorial data label the exponential terms of the tropical theta function that produces the associated KP multi-soliton.

Hirota varieties of banana graphs

Building on the combinatorial framework described in the previous section, we introduce the Hirota variety of a graph, which parametrizes τ-functions arising from tropical limits of Riemann theta functions satisfying the Hirota bilinear relations [4, 7]. This is equivalent to asking that the function

$$u(x, y, t) \;=\; 2\,\partial_x^2 \log \tau(x, y, t)$$

is a solution to the KP equation (1). For banana graphs, we describe the main component of this variety explicitly: Theorem 5.1 in [2] gives a parametrization in terms of tropical data that realizes all such τ-functions as KP multi-solitons. In this framework, the matroid underlying a KP soliton coincides with the matroid determined by the associated Voronoi vertex and graph orientation ([2, Corollary 5.4]). We further show that this parametrization agrees with previously known descriptions [1, 14] of KP multi-solitons arising from rational degenerations of hyperelliptic curves ([2, Theorems 5.10 and 5.14]). Finally, real and positive Hirota varieties are defined, relating them to totally nonnegative Grassmannians and MM-curves as in [1, 11]. Equivalently, the real and positive Hirota variety parametrizes real τ–functions of a graph satisfying Hirota bilinear relation with positivity constraints on their coefficients. This makes the positive Hirota variety a natural object from the viewpoint of positive geometry [12, 13, 15], providing a tropical realization of the structures underlying real and regular KP solitons.

Acknowledgements. The first author has been partially supported by HORIZON-MSCA-2022-SE-01-01 CaLIGOLA, COST Action CaLISTA CA21109, GNFM-INdAM, and INFN projects MMNLP and GAST. The third author has been partially supported by European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 101034255); and by the European Research Council (ERC) under the European Union's Horizon Europe research and innovation programme, grant agreement 101040794 (10000DIGITS). The fourth author has been partially supported by the National Science Foundation under Award DMS2402069, the UC President's Postdoctoral Fellowship Program, and the Bob Moses Fund of the Institute for Advanced Study.

References

[1] S. Abenda: On a family of KP multi-line solitons associated to rational degenerations of real hyperelliptic curves and to the finite non-periodic Toda hierarchy. *J. Geom. Phys.* **119**, 112–138 (2017).

[2] S. Abenda, T.Ö. Çelik, C. Fevola, Y. Mandelshtam: Tropical KP theory for banana curves. *ArXiv:2512.13366* (2026).

[3] S. Abenda, P.G. Grinevich: Real regular KP divisors on M-curves and totally non-negative Grassmannians. *Lett. Math. Phys.* **112**, 115 (2022).

[4] D. Agostini, C. Fevola, Y. Mandelshtam, B. Sturmfels: KP solitons from tropical limits. *J. Symbolic Comput.* **114**, 282–301 (2023).

[5] O. Amini: Lattice of integer flows and poset of strongly connected orientations. *ArXiv:1007.2456* (2010).

[6] B.A. Dubrovin, S.M. Natanzon: Real theta-function solutions of the Kadomtsev-Petviashvili equation. *Math. USSR-Izv.* **52**, 267–286 (1988).

[7] C. Fevola, Y. Mandelshtam: Hirota varieties and rational nodal curves. *J. Symbolic Comput.* **120**, 102239 (2024).

[8] T. Ichikawa: Periods of tropical curves and associated KP solutions. *Comm. Math. Phys.* **402**(2), 1707–1723 (2023).

[9] T. Ichikawa: Tropical curves and solitons in nonlinear integrable systems. *Chaos Solitons Fractals* **182**, 114748 (2024).

[10] Y. Kodama, L. Williams: KP solitons and total positivity for the Grassmannian. *Invent. Math.* **198**, 637–699 (2014).

[11] M. Kummer, B. Sturmfels, R. Vlad: Maximal Mumford curves from planar graphs. *Pure Appl. Math. Q.* **21**, 1689–1719 (2025).

[12] T. Lam: *An invitation to positive geometries*. Open problems in algebraic combinatorics, Proc. Sympos. Pure Math. **110**, 159–179. Amer. Math. Soc. (2024).

[13] T. Lam: Moduli spaces in positive geometry. *Matematiche (Catania)* **80**(1), 17–101 (2025).

[14] A. Nakayashiki: On reducible degeneration of hyperelliptic curves and soliton solutions. *SIGMA* **15**, 009 (2019).

[15] K. Ranestad, B. Sturmfels, S. Telen: What is positive geometry? *Le Matematiche* **80**(1), 3–16 (2025).

Partition identities and A_r surface singularities

P. Afsharijoo[◇*], P.D. González Pérez[*†], H. Mourtada[‡]

[◇] *Speaker at EACA 2026*

[*] *Departamento de Álgebra, Geometría y Topología, Universidad Complutense de Madrid*

[†] *Instituto de Matemática Interdisciplinar, Universidad Complutense de Madrid*

[‡] *CNRS, Institut de Mathématiques de Jussieu-Paris Rive Gauche, Université Paris Cité, Sorbonne Université*

pooneh.afsharijoo@cyu.fr, pgonzalez@mat.ucm.es, hussein.mourtada@imj-prg.fr

Abstract. We prove a family of partition identities involving integer partitions in three colors. The identities established in this paper are associated with the A_r surface singularities via the arc HP-series, which provides a measure of singularities of algebraic varieties defined using arc spaces.

Introduction

An (ordinary) partition λ of a positive integer n is a non-increasing sequence of positive integers $(\lambda_1 \geq \cdots \geq \lambda_\ell)$ such that $\lambda_1 + \cdots + \lambda_\ell = n$. The integers λ_i are called the parts of λ. We denote by $L(\lambda)$ the number of parts (that is, the length) of λ, and by $p(n)$ the total number of partitions of n. A fundamental family of partition identities for ordinary partitions, which plays a central role in this note, is given by Gordon's identities (see Theorem 1 in [5]):

Theorem (Gordon's identities). Given integers $r \geq 2$ and $1 \leq i \leq r$, let $\mathcal{B}_{r,i}(n)$ denote the set of partitions of n of the form $(\lambda_1, \ldots, \lambda_s)$, where $\lambda_j - \lambda_{j+r-1} \geq 2$ and at most $i-1$ parts equal to 1 and denote its cardinal by $B_{r,i}(n)$. Let $\mathcal{A}_{r,i}(n)$ denote the number of partitions of n into parts $\not\equiv 0, \pm i \pmod{2r+1}$ and denote its cardinal by $A_{r,i}(n)$. Then $A_{r,i}(n) = B_{r,i}(n)$ for all integers n.

Note that these identities generalize the Rogers-Ramanujan identities, which correspond to the case $r = 2$ in the above theorem, and played and important role in mathematics.

Let $c \geq 1$ be an integer. A partition is called *c-colored* if each part can appear in c different colors; that is, for every integer i, we distinguish c different copies of the part i, one for each color. For $c = 3$, we consider the three colors black, red, and green. We denote by i_b (respectively i_r and i_g) the part of i color black (respectively red and green). For instance, the 3-colored partitions of 2 are: $2_b, 2_r, 2_g, 1_b+1_b, 1_b+1_r, 1_b+1_g, 1_r+1_g, 1_r+1_r, 1_g+1_g$.

J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, V. Sotomayor (eds.): Proceedings of the XIX EACA, pp. 36-40 (2026).
ISBN: 978-84-09-87277-0

The 3-colored partitions are naturally in bijection with the monomials in the graded ring

$$\mathcal{S} := \mathbf{K}[x_i, y_i, z_i]_{i\geq 1}, \tag{1}$$

where $\mathbf{K}$ is a field of characteristic zero and the grading is defined by setting weight i to x_i, y_i and z_i, for $i \geq 1$. To each monomial in $\mathcal{S}$, one associates a 3-colored partition by assigning to x_i, y_i, and z_i a part of size i colored black, red, and green, respectively. For example, the 3-colored partition corresponding to the monomial $x_2^2 y_2 z_3 z_4$ is $4_g + 3_g + 2_r + 2_b + 2_b$.

The ring $\mathcal{S}$ appears when we study the arc spaces associated with subvarieties in the 3-dimensional affine space. Our main result is a family of 3-colored partition identities, which has been obtained in connexion with the study of the arc spaces of A_r surface singularities.

Arc spaces of A_r singularities and Hilbert-Poincaré series

We consider the polynomial $h_r := z^r - xy \in \mathbf{K}[x, y, z]$. For $r \geq 2$, the surface defined by $X_{r-1} = \{h_r = 0\}$ has, at the origin, what is called an A_{r-1}-singularity, which is a rational double point singularity. The arc space $X_{r-1,\infty}$ of X_{r-1} is the moduli space parameterizing the arcs on X_{r-1}. An arc γ is given by a tuple of power series

$$\gamma(t) = (x(t), y(t), z(t)) = (\sum x_i t^i, \sum y_i t^i, \sum z_i t^i) \in (\mathbf{K}[[t]])^3$$

satisfying $h_r(\gamma(t)) = 0$. Let us consider the expansion:

$$h_r(\gamma(t)) = \sum H_i t^i, \text{ with } H_i \in \mathbf{K}[x_j, y_j, z_j]_{0\leq j\leq i}.$$

The arc space $X_{r-1,\infty}$ is the scheme defined in the infinite-dimensional affine space with coordinates x_i, y_i, z_i for $i \geq 0$, by the equations $H_i = 0$, for $i\geq 0$. The ring of regular functions on $X_{r-1,\infty}$ is $\mathcal{A}_r = \mathbf{K}[x_i, y_i, z_i]_{i\geq 0}/(H_i)_{i\geq 0}$.

In order to describe the properties of the polynomials H_i, it is convenient to make a change of variables, replacing respectively x_i, y_i, z_i by $x_i/(i!), y_i/(i!), z_i/(i!)$ for $i \geq 1$. By convenience we denote also by H_i the transform of H_i after this change. The ring $\mathbf{K}[x_i, y_i, z_i]_{i\geq 0}$, is equipped with the derivation D given by $D(x_i) = x_{i+1}$, $D(y_i) = y_{i+1}$ $D(z_i) = z_{i+1}$. Then, we have that $H_0 = z_0^r - x_0 y_0$, and $H_i = D(H_{i-1})$ for $i \geq 1$, that is, the ideal $(H_i \mid i \in \mathbf{Z}_{\geq 0})$ is a differential ideal (*e.g.*, Proposition 2.3 in [7]). Each polynomial H_j is weighted homogeneous of weight j, when x_i, y_i, z_i is given weight i for $i \in \mathbf{Z}_{\geq 0}$.

We focus on the space of arcs γ satisfying $\gamma(0) = 0$. We denote it by $X^0_{r-1,\infty}$. Let us denote by by $\overline{H}_i \in \mathcal{S}$ the polynomial obtained from H_i by putting $x_0 = y_0 = z_0 = 0$ (where $\mathcal{S}$ is defined in (1)). The ring of functions on $X^0_{r-1,\infty}$ is the quotient $\mathcal{A}^0_r := \mathcal{S}/\mathfrak{a}_r$, where the ideal

$$\mathfrak{a}_r = (\overline{H}_i)_{i\in\mathbf{Z}_{\geq 1}} \subset \mathcal{S}$$

is weighted homogeneous. The ring $\mathcal{A}^0_r = \bigoplus_{j\in\mathbf{Z}_{\geq 0}} \mathcal{A}^0_{r,j}$ is naturally graded. The arc Hilbert Poincaré series (arc HP-series) of X_{r-1} at 0 is $\mathsf{AHP}_{X_{r-1},0}(q) := \sum_{j\in\mathbf{Z}_{\geq 0}} \dim_{\mathbf{K}} \mathcal{A}^0_{r,j}\, q^j$. By the geometry of the jet schemes of this particular surface singularity one has:

Theorem 1. ([8])

$$\mathsf{AHP}_{X_{r-1}}(q) = \frac{1}{1-q^3} \prod_{i\geq 2} \frac{1}{1-q^i}.$$

A conjecture on the initial ideal

We denote by $\mathrm{in}(\mathfrak{a}_r)$ the initial ideal of $\mathfrak{a}_r$ with respect to the weighted reverse lexicographic order in $\mathcal{S}$. The initial ideals $\mathrm{in}(\mathfrak{a}_r)$, even for a given value of r, are not easy to determine since $\mathfrak{a}_r$ is not finitely generated. We have used the computer algebra system `Singular` to study generators of the initial ideal $\mathrm{in}(\mathfrak{a}_r)$ at bounded degrees for some values of r. The following definition is based on these computations:

Definition 2. Let $I_r := (z_i^r, z_i^{r-1}z_{i+1}, \cdots, z_i z_{i+1}^{r-1} |\ i \geq 1)$ and denote by J_r the ideal generated by following monomials:

- The monomials of I_r;
- The monomials of the form
$$x_k y_{i_1} \cdots y_{i_k}$$
where $1 \leq k, 1 \leq i_1 \leq \cdots \leq i_k$ and $k + i_k \leq r - 1$;
- The monomials of the form
$$x_k y_{i_1} \cdots y_{i_k} z_{j_1} \cdots z_{j_{i_k+k-r+1}},$$
where $1 \leq k, 1 \leq i_1 \leq \cdots \leq i_k, 2 \leq j_1 \leq \cdots \leq j_{k+i_k-r+1}$ and $k + i_k \geq r$.

We have the following conjecture

Conjecture 3. *The initial ideal* $\mathrm{in}(\mathfrak{a})$ *is the ideal* J_r *defined above.*

Let J be a monomial ideal of $\mathcal{S}$. One associates to J the set of 3-colored partitions $\mathcal{F}_J$ defined by those monomials which are not zero in the ring $\mathcal{S}/J$. We denote by $\mathcal{F}_J(n)$ the set of partitions of n in $\mathcal{F}_J$. Then, the generating series of the sequence $F_J(n)$ is equal to the Hilbert series of $\mathcal{S}/J$, because the monomials of $\mathcal{S}$ of weight n which are not in J form a basis of the weighted-homogeneous component of $\mathcal{S}/J$ of weight n.

Definition 4. The partitions in $\mathcal{F}_r := \mathcal{F}_{J_r}$ are the 3-colored partitions associated with the monomials which are not in the ideal J_r. Let $F_r(n)$ denote the cardinality of $\mathcal{F}_r(n)$, the set of integer partitions of n belonging to $\mathcal{F}_r$.

Statement of the main result

For a 3-colored partition λ, we may consider the subpartitions λ_b, λ_r, and λ_g, obtained respectively from the black, red, and green parts of λ. For example, for the partition $\lambda = 7_b + 6_r + 3_b + 3_r + 1_r$, we have $\lambda_b = 7 + 3$, $\lambda_r = 6 + 3 + 1$, and $\lambda_g = \emptyset$. We denote by ℓ_b (respectively by ℓ_r and ℓ_g) the number of black (respectively red and green) parts of λ. We denote by k the smallest black part of λ, if it exists. If $\ell_r \geq k$, we denote by i_k the k-th smallest red part of λ.

Proposition 5. *The set* $\mathcal{F}_r$ *consists of the* 3*-colored partitions* λ *satisfying one of the following conditions:*

1. *Either $\lambda = \emptyset$ or all parts of λ are colored in a single color: black, red or green; and if this color is green, then $\lambda \in \mathcal{B}_{r,r}(n)$ of Gordon's identities for some positive integer n.*
2. *λ has two colors, either black and green or red and green, with green sub-partition λ_g belonging to $\mathcal{B}_{r,r}(n)$ of Gordon's identities for some integer n.*
3. *λ has two colors black and red, with*
   (a) *either $\ell_r \leq k-1$,*
   (b) *or $\ell_r \geq k$ and $k + i_k \geq r$.*
4. *λ has three colors (black, red and green) with green sub-partition λ_g belonging to $\mathcal{B}_{r,r}(n)$ of Gordon's identities for some integer n and with*
   (a) *either $\ell_r \leq k-1$,*
   (b) *or $\ell_r \geq k$ and $k + i_k \geq r$ with $\ell_g - \#\{1_g\} < k + i_k - r + 1$.*

Our main result is the following:

Theorem 6. *For all $n \in \mathbf{N}$ and all integers $r \geq 2$, the numbers $F_r(n)$ are equal:*

$$F_2(n) = F_3(n) = F_4(n) = \cdots .$$

Moreover, this common value equals the number of integer partitions of n in which the part 1 may appear in 3 colors, while all other positive integers may appear in 2 colors.

Remark 7. It is well-known that the Hilbert series of an ideal coincides with the Hilbert series of its initial ideal with respect to a monomial ordering that respects the grading (e.g., see [6], the appendix of [4]). It follows that the Hilbert series of $\mathcal{S}/\mathrm{in}(\mathfrak{a}_r)$ is equal to the Hilbert series of $\mathcal{S}/\mathfrak{a}$, which by definition is equal to $\mathrm{AHP}_{X_{r-1}}(q)$. It follows that if Conjecture 3 holds, then it implies Theorem 6. On the other hand, Theorem 6 provides a strong evidence for this conjecture.

The strategy to prove Theorem 6 passes by the computation of the generating series of $F_r(n)$ as the sum of the generating series of the four types of partitions in Proposition 5 (see [2] for details). The proof relies on several recent developments in combinatorics and differential algebra, see [1, 3, 4].

Acknowledgements. The first author has been funded by *María Zambrano Program*. The first and second authors have been funded by grants PID2020-114750GB-C32 and PID2024-156181NB-C32 of MICIU/AEI MCIN/AEI /10.13039/501100011033 and FEDER, UE.

References

[1] P. Afsharijoo, J. Dousse, F. Jouhet, H. Mourtada: New companions to the Andrews-Gordon identities motivated by commutative algebra. *Adv. Math.* **417**, 108946 (2023).

[2] P. Afsharijoo, P.D. González Pérez, H. Mourtada: Partition identities associated with A_r-surface singularities. *ArXiv:2601.12048* (2026).

[3] R. Ait El Manssour, G. Pogudin: Multiplicity structure of the arc space of a fat point. *Algebra Number Theory* **18**(5), 947–967 (2024).

[4] C. Bruschek, H. Mourtada, J. Schepers: Arc spaces and the Rogers-Ramanujan identities. *Ramanujan J.* **30**(1), 9–38 (2013).

[5] B. Gordon: A combinatorial generalization of the Rogers-Ramanujan identities. *Amer. J. Math.* **83**, 393–399 (1961).

[6] G.M. Greuel, G. Pfister: *A Singular introduction to commutative algebra*. Springer (2002).

[7] H. Mourtada: Jet schemes of complex plane branches and equisingularity. *Ann. Inst. Fourier* **61**(6), 2313–2336 (2011).

[8] H. Mourtada: *Jet schemes of rational double point surface singularities*. Valuation theory in interaction, EMS Ser. Congr. Rep., 373–388. Eur. Math. Soc. (2014).

Picard-Vessiot theory of spectral problems

C. Arreche*, S.L. Rueda◇†, J.A. Weil‡

◇ *Speaker at EACA 2026*

* *University of Texas at Dallas*

† *Universidad Politécnica de Madrid*

‡ *Université de Limoges*

arreche@utdallas.edu, sonialuisa.rueda@upm.es, jacques-arthur.weil@unilim.fr

Abstract. An algebro-geometric ordinary differential operator L is characterized by having a centralizer of rank 1 or equivalently an abelian differential Galois group of $L-\lambda$ in a Tannakian sense, for a generic λ. In this framework, we study the spectral problem $(L-\lambda)(y)=0$, to develop an effective Picard-Vessiot theory over a finite algebraic extension of the field of the spectral curve.

Commuting operators and spectral curves

Suppose (K,∂) is a differential field of characteristic zero with algebraically closed subfield of constants $C:=K^{\partial}$. The ring of differential operators $K[\partial]$ is a (left and right) non commutative Euclidean domain. Given differential operators $P,Q\in K[\partial]$, we denote a greatest common right divisor of P and Q by gcrd(P, Q).

Given an ordinary differential operator L in $K[\partial]\backslash C[\partial]$, the centralizer of L in $K[\partial]$,

$$\mathcal{Z}(L)=\{A\in K[\partial]\mid LA=AL\},$$

has no zero divisors. Moreover $\mathcal{Z}(L)$ it is a commutative domain by [5, Corollary 4.2]. To review the long history of this result, see for instance [5, Sections 3 and 4].

In most cases, the centralizer is trivial $\mathcal{Z}(L)=C[L]$, while spectral problems $(L-\lambda)(y)=0$ for differential operators L with non-trivial centralizers have very special properties. In every case, the quotient field of $\mathcal{Z}(L)$ is a function field in one variable, whose transcendence degree is one. Moreover any subalgebra $\mathcal{A}$ of $\mathcal{Z}(L)$ has Krull dimension one, it is the affine ring of an algebraic curve Spec($\mathcal{A}$). This fact was first proved by Burchnall and Chaundy [3], and in greater generality by Krichever [7], followed by Mumford [9]. In particular, the spectral curve is $\Gamma:=$ Spec($\mathcal{Z}$(L)), and we have an isomorphism [1]

$$\theta:\mathcal{Z}(L)\to\mathcal{O}_{\Gamma}(\Gamma).$$

J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, V. Sotomayor (eds.): Proceedings of the XIX EACA, pp. 41-45 (2026). ISBN: 978-84-09-87277-0

Algebro-geometric operators and parametric factorizations

In this presentation, we restrict to the very special case of algebro-geometric ordinary differential operators, whose definition is better understood in terms of the notion of rank.

Definition 1. For a differential operator $L \in K[\partial]$ the rank of a subalgebra $\mathcal{A}$ of $\mathcal{Z}(L)$ is defined as follows:

1. the gcd of the orders of the operators $A \in \mathcal{A}$ (see [10]);
2. the dimension of the space of common solutions of $Ay = \theta(A)y$ for $A \in \mathcal{A}$ (see [1]).

In contrast, the rank of $A, B \in \mathcal{Z}(L)$ is defined to be $\mathrm{rank}(A, B) := \gcd(\mathrm{ord}(A), \mathrm{ord}(B))$. It is important to note that $\mathrm{rank}(A, B) \geq \mathrm{rank}(\mathsf{C}[\mathsf{A}, \mathsf{B}])$ [10], and in general this inequality may be strict. The equivalence between the above definitions is clear in the rank 1 case but otherwise needs to be proved explicitly. This is done by Wilson in case $\mathcal{A} = C[A, B]$ in [14].

Definition 2. A differential operator $L \in K[\partial]$ is called algebro-geometric if any of the following equivalent conditions is satisfied:

1. there exists $A \in \mathcal{Z}(L)$ whose order is coprime with the order of L;
2. $\mathrm{rank}(\mathcal{Z}(\mathsf{L})) = 1$.

Let us denote by $C[\Gamma]$ the coordinate ring of the spectral curve $\mathcal{O}_\Gamma(\Gamma) \simeq \mathcal{Z}(L)$ and by $C(\Gamma)$ its fraction field. The next result can be proved following similar ideas to [4, Lem. 8.7], or one can give more direct proofs (at least in some special cases), generalizing [8]. With the natural extended derivation $\tilde{\partial}$, $K[\Gamma] := K \otimes C[\Gamma]$ is a differential domain, we will denote by $K(\Gamma)$ its fraction field.

Theorem 3. *1. The ring of constants of $(K[\Gamma], \tilde{\partial})$ is $C[\Gamma]$.*
2. The field of constants of $(K(\Gamma), \tilde{\partial})$ is $C(\Gamma)$.

Let $\mathcal{A}$ be a commutative subring of $K[\partial]$ such that $L \in \mathcal{A}$. Consequently, $\mathcal{A}$ is a $C[L]$-submodule of $\mathcal{Z}(L)$. Assuming $\mathrm{ord}(\mathsf{L}) = \mathsf{n}$, consider the classes X mod n of the orders of all elements of $\mathcal{A}$. It can be proved as in [5], Theorem 1.2, that X is an additive subgroup of the cyclic group of order n. Then $t = |X|$ divides n and for each $i \in X$, there exists $A_i \in \mathcal{A}$ order minimal, its order is minimal in the set of orders of elements in $\mathcal{A}$ congruent with $\mathrm{ord}(\mathsf{A_i})$ mod n. Furthermore $\{1, A_1, \ldots, A_t\}$ is a $C[L]$-basis of $\mathcal{A}$. Given $A_1, A_2 \in \mathcal{Z}(L)\backslash C[L]$ we have $C[L] \subset C[L, A_i] \subset C[L, A_1, A_2] \subset \mathcal{Z}(L)$. The next result is a generalization of [13], Theorem 12, see also [12].

Theorem 4. *Given an algebro-geometric differential operator L in $K[\partial]\backslash C[\partial]$, if there exists $A_1, A_2 \in \mathcal{Z}(L)\backslash C[L]$ such that $\mathrm{rank}(\mathsf{L}, \mathsf{A_i}) = 1$ and whose orders are different mod n then $\gcrd(\mathsf{L} - \lambda, \mathsf{A_1} - \mu_1) \equiv \gcrd(\mathsf{L} - \lambda, \mathsf{A_2} - \mu_2)$ over $K(\Delta)$, for $\Delta = \mathrm{Spec}\,\mathsf{C}[\mathsf{L}, \mathsf{A_1}, \mathsf{A_2}]$.*

The previous theorem implies that there is an intrinsic right factor $\mathcal{F} = \partial + \phi$ of $L - \lambda$ over the spectral curve $\Gamma = \mathrm{Spec}(\mathcal{Z}(\mathsf{L}))$ corresponding to the whole centralizer, thus $\phi \in K(\Gamma)$.

We can compute $\mathcal{F}$ using any $A \in \mathcal{Z}(L)\backslash C[L]$ order minimal such that rank(L, A) = 1, we may assume that A is the smallest possible order. The planar curve $\Gamma_{L,A} = \mathrm{Spec}(C[L, A])$ is defined by an irreducible polynomial $f(\lambda, \mu)$ in $C[\lambda, \mu]$. The first differential subresultant of $L - \lambda$ and $A - \mu$ can be used to compute a first order right factor over $K(\Gamma_{L,A})$, see [12],

$$\mathcal{F} = \mathrm{gcrd}(L - \lambda, A - \mu) = \partial - \phi(\lambda, \mu), \quad \phi \in K(\Gamma_{L,A})$$

Spectral Picard-Vessiot fields

We have the following Galoisian criterion to characterize when $L \in K[\partial]$ is algebro-geometric.

Theorem 5. ([1]) *$L \in K[\partial]$ is algebro-geometric if and only if the differential Galois group of $L - \lambda$ is abelian.*

The differential Galois group in the above result is defined from the Tannakian point of view. One of our main goals is to make more concrete their construction, developing algorithms from the point of view of classical differential algebra. In this presentation we focus on Pircard-Vessiot extensions, that are not classical [11] since fields of constants are not algebraically closed.

Given an algebro-geometric differential operator L in $K[\partial]\backslash C[\partial]$ and $A \in \mathcal{Z}(L)\backslash C[L]$ order minimal and such that rank(L, A) = 1 with $\Gamma_{L,A} = \mathrm{Spec}(C[L, A])$, defined by $f(\lambda, \mu) = 0$. Let Ψ be determined by $\partial(\Psi) = \phi\Psi$, where Ψ belongs to the differential closure of the field $K(\Gamma_{L,A})$.

Theorem 6. *Given an algebro-geometric differential operator L in $K[\partial]\backslash C[\partial]$, let Ψ be a solution of $(L-\lambda)(Y) = 0$ defined by $\partial(\Psi) = \phi\Psi$. Then Ψ is transcendental over $K(\Gamma_{L,A})$ and the field of constants of $K(\Gamma_{L,A})\langle\Psi\rangle$ is $C(\Gamma_{L,A})$.*

Proof. By Gauss's Lemma, f is irreducible as a polynomial in $K(\lambda)[\mu]$. Look at elements of $K(\Gamma_{L,A})$ as polynomials in $K(\lambda)[\mu]/(f)$, where (f) is the ideal generated by f in $K(\lambda)[\mu]$.

It is straightforward to prove that ϕ is not a logarithmic derivative of a $K(\Gamma_{L,A})$ radical and by [2], Theorem 5.1.2 the result follows. □

Remark 7. For analytic coefficients of L and on non-singular points of $\Gamma_{L,A}$, Ψ is the Baker-Akheizer function at each point of $\Gamma_{L,A}$ [7].

If ord(L) = n, we can assume w.l.o.g that $f(\lambda, y) = y^n - a_{n-2}(\lambda)y^{n-2} + \ldots + a_1(\lambda)y + a_0(\lambda)$ and divide by $y - \mu$ in $C(\Gamma_{L,A})[y]$ obtaining $f(\lambda, y) = g(y)(y - \mu) + f(\lambda, \mu)$ with a polynomial $g \in C(\Gamma_{L,A})[y]$ of degree $n - 1$ in y, that could be reducible.

Example 8. If ord(L) = 3 we can choose A such that $f(\lambda, y) = y^3 + a_1(\lambda)y + a_0(\lambda)$. Then $g(y) = y^2 + \mu y + \mu^2 + a_1(\lambda)$. The solutions of $g(y) = 0$ are $(-\mu \pm \sqrt{-3\mu^2 - 4a_1(\lambda)})/2$. If $a_1(\lambda) = 0$ then $y_i = \varepsilon^i\mu$ for $\varepsilon = (-1 + i\sqrt{3})/2$.

Consider the Galois closure $C(\overline{\Gamma}_{L,A})$ of $C(\Gamma_{L,A})$ for $g(y)=0$ and $F := K \otimes C(\overline{\Gamma}_{L,A})$. Generically, then the curve $\Gamma_{L,A}$ has degree n and we can consider $n-1$ conjugate solutions $y_2, \ldots, y_n$ in $C(\overline{\Gamma}_{L,A})$ of $g(y)=0$ over $C(\Gamma_{L,A})$ and set $y_1 = \mu$. Then

$$\phi_i := \phi(\lambda, y_i) \in F.$$

The next result is proved with the same strategy as Theorem 3.

Theorem 9. *The field of constants of $F := K \otimes C(\overline{\Gamma}_{L,A})$ is $C(\overline{\Gamma}_{L,A})$.*

Define solutions Ψ_i of $(L-\lambda)(Y)=0$ by $\partial(\Psi_i) = \phi_i \Psi_i$. The commutativity of L and A ensures that Ψ_i are eigenvectors of A for different eigenvalues. Consequently, $\{\Psi_i\}$ is a fundamental system of solutions of $(L-\lambda)(Y)=0$. The spectral Picard-Vessiot field of $L-\lambda$ is defined as

$$\mathcal{E}(L-\lambda) = F\langle \Psi_1, \ldots, \Psi_n \rangle.$$

We prove that the field of constants of $\mathcal{E}(L-\lambda)$ coincides with the field of constants of F.

In some situations, the field of constants is still $C(\Gamma_{L,A})$, as in the case of Schrödinger operators [8], $L = \partial^2 + u$ with $u \in K$, where $\mathcal{Z}(L) = C[L, A]$ and $f(\lambda, \mu) = \mu^2 + a_0(\lambda)$. The solutions of $f(\lambda, y) = 0$ over $C(\Gamma)$ are $y_1 = \mu$ and $y_2 = -\mu$. Thus, we can take $F = K(\Gamma)$. Finally, the spectral Picard-Vessiot extension of $K(\Gamma)$ for $(L-\lambda)(Y)=0$ is $\mathcal{E}(L-\lambda) = K(\Gamma)\langle \Psi^1, \Psi^2 \rangle = K(\Gamma)\langle \Psi^i \rangle$ because $\Psi^1 \Psi^2 \in K(\Gamma)$.

Example 10. (Rational spectral curve) In the case of rational curves, $C(\Gamma) \simeq C(\tau)$, where τ is a free algebraic parameter over C. Consider $K = \mathbb{C}\langle \eta \rangle$, $\eta := \cosh(x)$, $\partial = d/dx$. Given $L = 12\eta' \eta^{-3} + 6\eta^{-2}\partial + \partial^3$, we computed $\mathcal{Z}(L) = C[L, A_1, A_2]$, $\mathrm{ord}(\mathsf{A}_1) = 4$, $\mathrm{ord}(\mathsf{A}_2) = 5$ using the algorithm in [6]. The spectral curve Γ of $C[L, A_1]$ is defined by

$$f_1(\lambda, \mu) = \lambda^4 - \mu^3 - 4\lambda^2 \mu - \frac{64}{27}\lambda^2 = 0$$

computed as the differential resultant $f_1 = \partial\mathrm{Res}(L-\lambda, A_1 - \mu)$ and parametrized by $\chi(\tau) = (\chi_1(\tau), \chi_2(\tau)) = (\tau^3, \tau^4 - (4/3)\tau^2)$. For a primitive third root of unity ε, $\phi_i := \phi(\chi(\varepsilon^i \tau))$, $i = 0, 1, 2$ determine the fundamental system of solutions $\{\Psi_1, \Psi_2, \Psi_3\}$ of $(L-\lambda)(y) = 0$ over $C(\tau)$. In this case $\mathcal{E}(L-\lambda) = K(\tau)\langle \Psi_1, \Psi_2, \rangle$ whose field of constants is $C(\tau)$.

Acknowledgements. The first and second author were partially supported by grant PID2021-124473NB-I00, «Algorithmic Differential Algebra and Integrability» (ADAI) from the Spanish MCIN/AEI /10.13039/501100011033 and by FEDER, UE. The third author would like to thank the Dpto. Matemática Aplicada UPM, for financing participation in ADAI International Workshop.

References

[1] A. Braveman, P. Etingof, D. Gaitsgory: Quantum integrable systems and differential Galois theory. *Transform. Groups* **2**, 31–56 (1997).

[2] M. Bronstein: *Symbolic integration I: Transcendental functions*. Springer (2013).

[3] J.L. Burchnall, T.W. Chaundy: Commutative ordinary differential operators. *Proc. Lond. Math. Soc.* **s2-21**, 420–440 (1923).

[4] H. Gillet, S. Gorchinskiy, A. Ovchinnikov: Parameterized Picard–Vessiot extensions and Atiyah extensions. *Adv. Math.* **238**, 322–411 (2013).

[5] K.R. Goodearl: Centralizers in differential, pseudo-differential and fractional differential operator rings. *Rocky Mountain J. Math.* **13**(4), 573–618 (1983).

[6] A. Jiménez-Pastor, S.L. Rueda: Effective computation of centralizers. *ArXiv:2505.01289* (2025).

[7] I.M. Krichever: Commutative rings of ordinary linear differential operators. *Funct. Anal. Appl.* **12**(3), 175–185 (1978).

[8] J.J. Morales-Ruiz, S.L. Rueda, M.A. Zurro: Spectral Picard–Vessiot fields for algebro-geometric Schrödinger operators. *Ann. Inst. Fourier* **71**(3), 1287–1324 (2021).

[9] D. Mumford: *An algebro-geometric construction of commuting operators and of solutions to the Toda lattice equation, Korteweg de Vries equation and related non-linear equations.* Proc. Int. Symp. Alg. Geom. (Kyoto, 1977), 115–153 (1978).

[10] E. Previato, S.L. Rueda, M.A. Zurro: Commuting ordinary differential operators and the Dixmier test. *SIGMA* **15**, 101 (2019).

[11] M. van der Put, M.F. Singer: *Galois theory of linear differential equations.* Grundlehren der Mathematischen Wissenschaften **328**, Springer (2012).

[12] S.L. Rueda: *On the classification of centralizers of ODOs: An effective differential algebra approach.* Functor and Tensor Categories, Models and Systems. Springer (2025).

[13] S.L. Rueda, M.A. Zurro: Spectral curves for third-order ODOs. *Axioms* **13**(4), 274 (2024).

[14] G. Wilson: *Algebraic curves and soliton equations.* Geometry Today, Progr. Math. **60**, 303–329. Birkhäuser (1985).

Algebraic cryptanalysis of DME schemes via determinantal ideals

M. Avedaño*, P. Coscojuela◇*, I. Luengo*
◇ *Speaker at EACA 2026*
* *Universidad Complutense de Madrid*
mavend01@ucm.es, picoscoj@ucm.es, iluengo@ucm.es

Abstract. We propose a systematic approach to analyzing the security of the family of DME cryptosystems, which belong to the area of multivariate cryptography. We focus on the DME scheme proposed to the NIST in 2023 and a minus variation of the scheme, called DME$^-$. As in many attacks on other multivariate cryptosystems, the bottleneck of the attack reduces to solving an instance of the MinRank problem of low rank, arising from the structure of the scheme. We prove that the expected number of solutions of such a MinRank instance is finite.

All complexity estimates are derived using existing results about complexity generalized determinantal ideals, and therefore rely on the assumption of genericity. Once the set of private keys is simplified –by specializing some of the variables– so that, for a given public key, there exists essentially a unique private key, the genericity assumption appears reasonable in light of the experimental results.

Introduction

The development by Shor in 1994 of an algorithm that can solve the underlying mathematical problems of the classical public-key cryptosystems –RSA and DSA– in polynomial time on a quantum computer, together with recent advances in building quantum hardware, has created an urgent need to develop new schemes that are resistant to quantum attacks.

The design of public-key schemes that remain secure against quantum computers is known as post-quantum cryptography. Its relevance beyond academia became evident when, in 2016, the National Institute of Standards and Technology (NIST) announced a call for proposals for quantum-resistant standards. Submissions to that call fall into five main classes: lattice-based, code-based, multivariate, isogeny-based and hash-based (the last only for digital signatures) public-key cryptography. Multivariate public-key cryptosystems are those in which the public key is given by a set of multivariate polynomials over a finite field. The fact that solving a system of randomly chosen multivariate polynomials over a finite field, with degree greater than one, is NP-hard, together with the expectation that quantum computers are unlikely to provide an advantage for this specific problem, makes multivariate schemes

J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, V. Sotomayor (eds.): Proceedings of the XIX EACA, pp. 46-49 (2026).
ISBN: 978-84-09-87277-0

attractive candidates for post-quantum primitives. Compared to lattice-based schemes, multivariate schemes generally have larger public keys. If

$$p_1, \ldots, p_m \in \mathbb{F}_q[X_1, \ldots, X_n],$$

where $\mathbb{F}_q$ is a finite field, are the public key polynomials of a multivariate scheme, then to send a message $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{F}_q^n$ to Bob, Alice computes

$$c_j = p_j(a_1, \ldots, a_n) \qquad j = 1, \ldots, m$$

and transmits the ciphertext $\mathbf{c} = (c_1, \ldots, c_m) \in \mathbb{F}_q^m$ to Bob.

Bob's secret key is a trapdoor: information that allows him to recover **a** from **c** efficiently. Consequently, the system of polynomial equations formed by the public-key polynomials must have some special structure. The NP-hardness of solving random systems of polynomial equations of degree greater than one therefore does not guarantee that systems with the particular structure induced by a cryptosystem are also hard to solve.

Because the public key is a set of polynomials, *algebraic cryptanalysis* –attacks that attempt to solve systems of polynomial equations derived from the scheme's structure– is especially relevant to multivariate schemes. Gröbner-basis computation is a central tool for such attacks. However, the average-case complexity of computing a Gröbner basis is exponential in the number of variables, and its worst-case complexity is doubly exponential.This explains the interest in understanding the performance of Gröbner-basis algorithms on systems that arise in cryptography: complexity estimates are often given for generic systems and provide upper bounds for Gröbner-basis computation. Equations produced by concrete schemes typically exhibit additional algebraic structure that can be exploited; consequently, systems that appear intractable according to generic-parameter estimates may become solvable in practice.

DME schemes have a layered construction –typical of secret-key schemes– that combines linear (or affine) maps with a class of nonlinear maps known as *monomial maps* in algebraic geometry; we will refer to these as *exponential maps*. Unlike many other multivariate candidates, the public-key polynomials in DME have very high degree but are very sparse, which keeps the public-key size reasonable. The DME scheme defined in [5] adds some linear relations in the entries of the exponential maps, which eliminate the syzygies used in [2]. Additionally, only the structure of the matrices that define the nonlinear maps is public, not the exact values of their entries. A new structural attack on an instance of this version was later found in [3]. They were able to first compute equivalent matrices for the nonlinear maps and then recover the linear maps layer by layer by computing Gröbner bases of systems derived from the scheme. For details on DME schemes see [1].

This led us to consider further modifications: the DME$^-$ versions, which are obtained by applying the "minus" modification (used previously in schemes such as Imai–Matsumoto to prevent Patarin's linearization attack): some of the public polynomials are removed from the public key. Analogous systems of equations –now over $\mathbb{F}_q$– can be derived from the public polynomials of the minus versions to recover an equivalent private key.

The results of this submission appeared on [4].

Notation

In the following $q = 2^k$ for $k \in \mathbb{Z}$, $\mathbb{F}_q$ will denote the finite field of q elements. The finite field $\mathbb{F}_{q^2}$ will be sometimes regarded as a vector space over $\mathbb{F}_q$ with basis $\{1, u\}$.

MinRank modelling of the DME/DME$^-$ structural attack

Although the systems of equations arising from DME and DME$^-$ are similar, the corresponding solving strategies differ. In the original DME scheme, once **L** is recovered, one can compute $(\mathbf{L} \circ \mathbf{E})^{-1}(\mathbf{c})$. In the DME-minus variant, the ciphertext is $\mathbf{c}^-$, obtained from **c** by removing certain components. Hence, recovering **L** is no longer sufficient; a different reconstruction strategy is required.

We introduce a framework to systematically analyze the complexity of structural attacks against the two versions of DME. We show that the bottleneck of these attacks is the computation of Gröbner bases of certain *generalized determinantal ideals*, that is, ideals generated by all minors of a fixed order of a matrix whose entries are multivariate polynomials. More precisely:

- For the DME scheme, we prove that the associated determinantal ideal is generated by the 2×2 minors of a matrix **M** whose entries are affine linear forms. We denote this ideal by $\mathcal{I}_{\text{Minors}(2),\mathbf{M}}$.
- For the DME-minus scheme, the corresponding ideal is generated by the 3×3 minors of a matrix **M** whose entries are affine linear forms. We denote this ideal by $\mathcal{I}_{\text{Minors}(3),\mathbf{M}}$.

Complexity results for computing Gröbner bases of generalized determinantal ideals are given in [6, Chapter 3]; these results apply to generic instances. Although one might expect the determinantal ideals arising from DME or DME$^-$ instances to be non-generic, our experiments indicate that they have the expected dimension.

This allows us to derive upper bounds on the complexity. However, in order to recover the solutions explicitly, it is desirable for the ideal to be zero-dimensional. This is established in the next section.

Zero-dimensional instances and complexity estimates

The main results of this section are as follows:

- For the DME scheme, the determinantal ideal $\mathcal{I}_{\text{Minors}(2),\mathbf{M}}$ is zero-dimensional, as predicted by the theoretical analysis. Consequently, the system of equations to be solved simplifies drastically and takes the form
$$\{A_i^{2^e} C_j^{2^f} = R_{ij}\}_{ij},$$
where A_i, C_j, and $R_{ij} \in \mathbb{F}_{q^2}$ are known values, and $e, f \in \mathbb{Z}$ are also known.

- For the DME$^-$ scheme, the ideal $\mathcal{I}_{\text{Minors}(3),\mathbf{M}}$ typically has positive dimension. However, after concatenating two matrices $\mathbf{M}_1$ and $\mathbf{M}_2$ corresponding to two distinct systems of equations in a suitable way, the resulting ideal becomes zero-dimensional. This leads to simpler systems of equations of the form

$$\{[(a_i + ub_i)^{2^e}(c_j + ud_j)^{2^f}]_1 = r_{ij}\}_{ij},$$

where $[.]_1$ denotes the first coordinate of an element of $\mathbb{F}_{q^2}$, viewed as a vector space over $\mathbb{F}_q$ with basis $\{1, u\}$. Here $a_i, b_i, c_j, d_j \in \mathbb{F}_q$ are unknowns, $r_{ij} \in \mathbb{F}_q$ are known values, and $e, f \in \mathbb{Z}$ are also known.

How to reduce the complexity?

Building on [6], we observe that, in general, the complexity of computing a Gröbner basis of a generic generalized determinantal ideal is exponential in the number of equations and variables. For the systems arising from DME schemes we present a method that drastically reduces the support of the public-key polynomials. This reduction decreases both the number of variables and the number of equations in the derived systems. If the reduction is excessive, however, the generalized determinantal ideal may become positive-dimensional over $\overline{\mathbb{F}_q}$, making it difficult to extract solutions over $\mathbb{F}_q$. We therefore need to establish a trade-off between reducing the system size and preserving zero-dimensionality.

References

[1] M. Avendaño: *The DME cryptosystem*. `https://blogs.mat.ucm.es/dme/` (2025).

[2] M. Avendaño, M. Marco: A structural attack to the DME-$(3, 2, q)$ cryptosystem. *Finite Fields Appl.* **71**, 101810 (2021).

[3] P. Briaud, M. Bros, R. Perlner, D. Smith-Tone: *Practical attack on all parameters of the DME signature scheme*. Annual International Conference on the Theory and Applications of Cryptographic Techniques, 3–29. Springer (2024).

[4] P. Coscojuela Escanilla: *Security analysis of the family of DME schemes*. Universidad Complutense de Madrid (2026).

[5] I. Luengo, M. Avendaño, P. Coscojuela: *DME: A full encryption, signature and KEM multivariate public key cryptosystem*. Post-Quantum Cryptography, 379–402. Springer (2023).

[6] P.J. Spaenlehauer: *Solving multi-homogeneous and determinantal systems: algorithms, complexity, applications*. PhD thesis, Université Pierre et Marie Curie (2012).

Finite-dimensional directed graphs inducing Tortkara algebra structures

J. Baena Gómez[◇*], M. Ceballos González[†], D. Fernández Ternero[*]

[◇] *Speaker at EACA 2026*

[*] *Dpto. Geometría y Topología, Universidad de Sevilla*

[†] *Dpto. de Ingeniería, Universidad Loyola Andalucía*

jesbaegom@alum.us.es, mceballos@uloyola.es, desamfer@us.es

Abstract. In this paper, we investigate the relationship between Tortkara algebras and combinatorial structures from a graph-theoretic perspective. We characterize the structural conditions that such combinatorial objects must satisfy in order to be associated with low-dimensional Tortkara algebras. This approach provides a combinatorial framework that allows us to describe and analyze these algebras in terms of their underlying discrete structures.

Introduction

Tortkara algebras form a class of non-associative algebras introduced by Dzhumadil'daev, A. S. in [1]. It was shown there that the commutator algebra of any Zinbiel algebra is a Tortkara algebra, thereby establishing a natural connection between these two algebraic structures.

The main objective of this work is to explore the interplay between Graph Theory and Tortkara algebras, following the line of research developed in [2, 3] for Leibniz and Zinbiel algebras. Our aim is to extend this combinatorial viewpoint to the Tortkara setting and to determine the graph-theoretic properties that correspond to low-dimensional Tortkara algebra structures.

Preliminaries

We show some preliminary concepts on Tortkara algebras.

Definition 1. A Tortkara algebra $\mathcal{T}$ over a field $\mathbb{K}$ is a vector space with a bilinear product which satisfies

$$xx = 0,\ \forall x \in \mathcal{T}, \tag{1}$$

$$(xy)(zy) = J(x,y,z)y, \text{ where } J(x,y,z) = (xy)z + (yz)x + (zx)y,\ \forall x,y,z \in \mathcal{T}. \tag{2}$$

The latter is called the Tortkara identity.

Corollary 2. *A Tortkara algebra is anticommutative (i.e. $xy = -yx, \forall x, y \in \mathcal{T}$).*

J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, V. Sotomayor (eds.): Proceedings of the XIX EACA, pp. 50-54 (2026).
ISBN: 978-84-09-87277-0

Proposition 3. *Over a field of characteristic different from two, the Tortkara identity has the following multi-linear form*

$$(xy)(zw) + (xw)(zy) = J(x,y,z)w + J(x,w,z)y,\ \forall x,y,z,w \in \mathcal{T}. \tag{3}$$

From now on, we use the notation

$$T(x,y,z,w) = (xy)(zw) + (xw)(zy) - J(x,y,z)w - J(x,w,z)y.$$

Definition 4. Given a basis $\{e_i\}_{i=1}^n$ of an n-dimensional Tortkara algebra $\mathcal{T}$, its structure constants are defined by $e_ie_j = \sum_{h=1}^{n} c_{i,j}^h e_h$, for $1 \leq i,j \leq n$.

Definition 5. The derived series of a finite-dimensional Tortkara algebra $\mathcal{T}$ is

$$\mathcal{T}_1 = \mathcal{T},\ \mathcal{T}_2 = \mathcal{T}\mathcal{T},\ \mathcal{T}_3 = \mathcal{T}_2\mathcal{T}_2,\ \ldots,\ \mathcal{T}_k = \mathcal{T}_{k-1}\mathcal{T}_{k-1},\ \ldots$$

$\mathcal{T}$ is $(m-1)$-step solvable if there exists $m \in \mathbb{N}$ such that $\mathcal{T}_m = \{0\}$ and $\mathcal{T}_{m-1} \neq \{0\}$.

Definition 6. The central series of a finite-dimensional Tortkara algebra $\mathcal{T}$ is

$$\mathcal{T}^1 = \mathcal{T},\ \mathcal{T}^2 = \mathcal{T}\mathcal{T},\ \mathcal{T}^3 = \mathcal{T}^2\mathcal{T},\ \ldots,\ \mathcal{T}^k = \mathcal{T}^{k-1}\mathcal{T},\ \ldots$$

$\mathcal{T}$ is $(m-1)$-step nilpotent if there exists $m \in \mathbb{N}$ such that $\mathcal{T}^m = \{0\}$ and $\mathcal{T}^{m-1} \neq \{0\}$.

Associating combinatorial structures with Tortkara algebras

Let $\mathcal{T}$ be a n-dimensional Tortkara algebra with basis $\mathcal{B} = \{e_i\}_{i=1}^n$ and whose structure constants correspond to $e_ie_j = \sum_{h=1}^n c_{i,j}^h e_h$. Then, the pair $(\mathcal{T},\mathcal{B})$ is associated with a combinatorial structure by the following procedure:

a) For each $e_i \in \mathcal{B}$, we draw a vertex i.
b) Given two vertices i, j with $i < j$ verifying $c_{i,j}^j \neq 0$, we draw a directed edge from vertex i to j with weight $c_{i,j}^j$. Also, if $c_{i,j}^i \neq 0$, we draw a directed edge from vertex j to i with weight $c_{i,j}^i$.
c) Given three vertices $i < j < k$ such that $(c_{i,j}^k, c_{j,k}^i, c_{i,k}^j) \neq (0,0,0)$, we draw a full triangle ijk such that the edges ij, jk and ik have weights $c_{i,j}^k$, $c_{j,k}^i$ and $c_{i,k}^j$, respectively. Moreover:

   c1) We use a discontinuous line (named *ghost edge*) for edges with weight 0.
   c2) If two triangles ijk and ijl with $i < j < k < l$ satisfy $c_{i,j}^k = c_{i,j}^l$, draw only one edge between vertices i and j shared by both triangles.

Digraphs and Tortkara algebras

We study the digraphs associated with Tortkara algebras. Let $\mathcal{T}$ be a Tortkara algebra with basis $\mathcal{B} = \{e_i\}_{i=1}^n$ such that the combinatorial structure G associated with $(\mathcal{T},\mathcal{B})$ consists of a digraph; that is, there are no triangles in G. The law of $\mathcal{T}$ is given by

$$\begin{gathered} e_ie_j = c_{i,j}^i e_i + c_{i,j}^j e_j = -e_je_i,\ 1 \leq i < j \leq n, \\ e_ke_k = 0,\ 1 \leq k \leq n. \end{gathered} \tag{4}$$

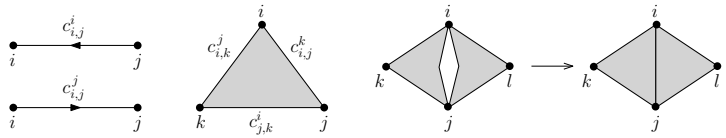


Figure 1. Directed edge, full triangle and two triangles sharing an edge.

The only possible digraph G with 1 vertex is formed by an isolated vertex and it is associated with the unique 1-dimensional Tortkara algebra, which is abelian.

Proposition 7. *Let G be a digraph of 2 vertices associated to a 2-dimensional Tortkara algebra $\mathcal{T}$ with basis $\mathcal{B} = \{e_i\}_{i=1}^2$. Then, G can be isomorphic to every possible configuration, which are shown in Figure 2, if and only if all edges have non-zero weight.*

Proposition 8. *Under the assumptions in Proposition 7, it is verified that*

- *Configuration $a)$ is associated with the abelian 2-dimensional Tortkara algebra.*
- *Configurations $b)$ and $c)$ are associated to 2-step solvable, non-nilpotent Tortkara algebras.*

Proposition 9. *Let G be a non-connected digraph of 3 vertices associated to a 3-dimensional Tortkara algebra $\mathcal{T}$ with basis $\mathcal{B} = \{e_i\}_{i=1}^3$. Then, G can be isomorphic to every possible configuration, which are shown in Figure 3, if and only if all edges have non-zero weight.*

Proposition 10. *Under the assumptions in Proposition 9, it is verified that*

- *Configuration $i)$ is associated with the abelian 3-dimensional Tortkara algebra.*
- *Configurations $ii)$ and $iii)$ are associated to 2-step solvable, non-nilpotent Tortkara algebras.*

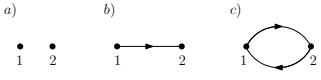


Figure 2. Digraphs with two vertices.

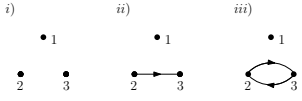


Figure 3. Disconnected digraphs with three vertices.

Proposition 11. *Let G be a connected digraph of 3 vertices associated to a 3-dimensional Tortkara algebra $\mathcal{T}$ with basis $\mathcal{B} = \{e_i\}_{i=1}^3$. Then, G cannot be isomorphic to configurations $7), 11)$ and $12)$ shown in Figure 4. Any other configuration is associated to a Tortkara algebra if and only if all edges have non-zero weight and, in case of configuration $13)$, it must also satisfy $c^1_{1,2} = -\dfrac{c^2_{1,2}c^1_{1,3}c^3_{2,3}}{c^3_{1,3}c^2_{2,3}}$.*

Proposition 12. *Under the assumptions in Proposition 11, all valid configurations are associated to solvable, non-nilpotent Tortkara algebras. More precisely:*

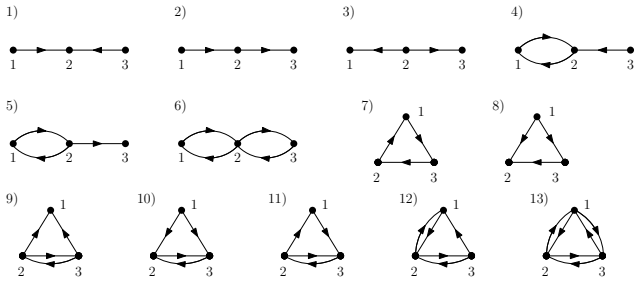


Figure 4. Connected digraphs with three vertices.

- $1)$ *and* $3)$ *are associated to* 2*-step solvable algebras.*
- $2), 4), 5), 6), 8), 10)$ *are associated to* 3*-step solvable algebras.*
- $9)$ *is associated to a* 2*-step solvable algebra if* $c^1_{1,2} = -\dfrac{c^1_{1,3}c^3_{2,3}}{c^2_{2,3}}$*. Otherwise, it is* 3*-step solvable.*
- $13)$ *is associated to a* 2*-step solvable algebra if* $c^2_{1,2} = c^3_{1,3}$ *and* $c^2_{2,3} = c^1_{1,3}$*. Otherwise, it is* 3*-step solvable.*

Algorithm for the Tortkara identity

We have developed an algorithmic procedure used in the previous section to evaluate the Tortkara identity and find out the forbidden and allowed configurations. We start considering a vector space $\mathcal{T}$ with basis $\mathcal{B}$ and the law expressed in (4). We have implemented our algorithm using the symbolic computation package MAPLE 22 following these steps:

1. Computing the product between two arbitrary basis vectors in $\mathcal{B}$.
2. Evaluating the product between two vectors expressed as a linear combination of vectors from $\mathcal{B}$.
3. Imposing the multi-linear form of the Tortkara identity (Equation 3) to every possible combination of elements of $\mathcal{B}$ and solving the corresponding system of equations.

The code can be found in `https://github.com/Jebago97/Tortkara`.

Acknowledgements. First and third authors have been partially supported by MICINN Spain Research Project MTM-PID2023-149804NB-I00. All authors has been partially supported by grant SOL2024-30793 (PPI 2024-25 Universidad de Sevilla).

References

[1] A.S. Dzhumadil'daev: Zinbiel algebras under q-commutators. *J. Math. Sci.* **144**(2), 3909–3925 (2007).

[2] M. Ceballos, J. Núñez, A.F. Tenorio: Finite-dimensional Leibniz algebras and combinatorial structures. *Commun. Contemp. Math.* **20**(1), 1750004 (2018).

[3] M. Ceballos, J. Núñez, A.F. Tenorio: Finite-dimensional Zinbiel algebras and combinatorial structures. *An. Ştiinţ. Univ. Ovidius Constanţa* **30**(3), 67–96 (2022).

Computing generalized additive decompositions via Hankel operators

E. Barrilli*, B. Mourrain*, D. Taufer◇†

◇ *Speaker at EACA 2026*

* *Inria at Université Côte d'Azur*

† *NUMA research unit at KU Leuven*

enrica.barrilli@inria.fr, bernard.mourrain@inria.fr, daniele.taufer@kuleuven.be

Abstract. We address the problem of computing minimal GADs of a given symmetric tensor through its associated linear operators. We prove that their Hankel operators encode the tensor's geometric structure, which can be used to retrieve minimal decompositions under suitable regularity assumptions. Within this framework, we further establish the uniqueness of such a minimal GAD and present a numerical routine for computing it.

Introduction

Symmetric tensors are ubiquitous objects that have attracted considerable attention from the algebraic and geometric communities. Their minimal decompositions have been thoroughly investigated from both symbolic and numerical perspectives, as they provide compact and insightful representations that reveal intrinsic structural properties. This has been successfully exploited in theoretical areas such as complexity theory and statistics, as well as in applied domains including data analysis, quantum physics, and signal processing.

Order-d symmetric tensors over an $(n+1)$-dimensional $\Bbbk$-vector space, with $\mathrm{char}(\Bbbk) = 0$, may be conveniently identified with homogeneous degree-d polynomials $\Bbbk[x_0, \dots, x_n]_d$. Here, we consider a general type of additive decomposition of a degree-d form f as

$$f = \sum_{i=1}^{s} \omega_i \ell_i^{d-k_i}, \tag{1}$$

where the ℓ_i's are non-proportional linear forms, which do not divide the corresponding degree-k_i form ω_i. These decompositions are known as (*reduced*) *generalized additive decompositions* [6], and will be shortened as *GAD*s of f.

In this work [2], we address the problem of computing *minimal* GADs for a given f. Precisely, we seek decompositions that minimize the GAD-rank, i.e., the weighted number of terms appearing in eq. (1), denoted by $\mathrm{rk}_{\mathsf{GAD}}(f)$. The weight of each $\omega_i \ell_i^{d-k_i}$ is given by the length of its naturally associated apolar scheme [3, 4]. When $k_i = d$ for every $i = 1, \dots s$, it reduces to the renowned *Waring decomposition problem*, and such a minimal Waring rank

J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, V. Sotomayor (eds.): Proceedings of the XIX EACA, pp. 55-59 (2026).
ISBN: 978-84-09-87277-0

s is known for *generic* [1] or special [7] choices of f. In general, $\mathrm{rk}_{\mathrm{GAD}}(f)$ is expected to be lower than the Waring rank, as GADs may possibly involve terms that are more structured than pure powers. Computing minimal GADs is a challenging task even in the *local* case (i.e., when $s = 1$), as terms of minimal weights display rich geometric configurations [9].

Differential operators associated with GADs

To each GAD term $\omega \ell^{d-k}$, we can associate a differential operator as follows. For any choice of linear forms $\mathbf{v} = (v_1, \ldots, v_n)$ that complete $\{\ell\}$ to a basis of $\Bbbk[x_0, \ldots, x_n]_1$, we consider the unique ℓ-expansion $\omega = \sum_{j=0}^{k} \omega_j(\mathbf{v})\ell^{k-j}$, and we use its polynomial coefficients to define $\omega^{d,\ell,\mathbf{v}} = \sum_{j=0}^{k}(d-j)!\,\omega_j(\mathbf{v})$. By using a set of linear forms $\mathbf{v}$ that is linearly independent with *every* ℓ_i, we define the operator associated with the GAD of eq. (1) as

$$\varphi = \sum_{i=1}^{s} \omega_i^{d,\ell_i,\mathbf{v}}(\partial) e^{\ell_i}(\partial) \in \Bbbk[[\partial]] \simeq \mathsf{Hom}(\Bbbk[x_0, \ldots, x_n], \Bbbk),$$

where the argument ∂ denotes the evaluation $x_i \mapsto \partial_{x_i}$, and $e^{\ell} = \sum_{k\in\mathbb{N}} \frac{\ell^k}{k!}$ is the usual exponential series. φ is a *polynomial-exponential series* [8], whose degree-d part $\varphi^{[d]}$ represents the differential action of f, namely, the operator $f^* : \Bbbk[x_0, \ldots, x_n]_d \to \Bbbk,\ p \mapsto f(\partial)(p)$.

Lemma 1. *Let $\varphi \in \Bbbk[[\partial]]$ as above. Then $f^* = \varphi^{[d]}$.*

Moreover, the operator φ can be used to recover the homogeneous ideal defining the projective zero-dimensional apolar scheme evinced by this GAD [4] as

$$I_\varphi = \mathsf{Ann}^\star(\varphi) = \{q \in \Bbbk[x_0, \ldots, x_n] \ :\ q \star \varphi = 0\},$$

where $q \star \varphi$ is the linear operator defined by $p \mapsto \varphi(pq)$. This yields a construction of such apolar schemes that relies only on linear algebra, improving upon previous homogenization methods [3, 4]. This connection is made explicit in [9, S 2.2]. Furthermore, the local lengths of these schemes, namely, the weight of each term $\omega_i \ell_i^{d-k_i}$, can be retrieved as the dimension of the $\Bbbk$-vector space spanned by all the derivatives of $\omega_i^{d,\ell_i,\mathbf{v}}$, i.e., its *inverse system*:

$$\langle\langle \omega_i^{d,\ell_i,\mathbf{v}} \rangle\rangle = \big\langle g(\partial)(\omega_i^{d,\ell_i,\mathbf{v}}) \ :\ g \in \Bbbk[\mathbf{v}] \big\rangle.$$

The next result shows that the dimension of inverse systems does not depend on d or $\mathbf{v}$.

Proposition 2. *For every $d \geq k$ and every choice of $\mathbf{v}, \mathbf{v}'$ as above, there is an isomorphism of $\Bbbk$-vector spaces*

$$\langle\langle \omega_i^{d,\ell_i,\mathbf{v}} \rangle\rangle \simeq \langle\langle \omega_i^{k_i,\ell_i,\mathbf{v}'} \rangle\rangle,$$

which respects the polynomial degree.

Computing minimal GADs

We study GADs through the use of the *Hankel operators* of the associated functionals φ. It is not restrictive to assume that the considered supports are of the form $\ell_i = x_0 + \sum_{j=1}^{n} \ell_{ij} x_j$.

Let $\mathcal{A}$ be a $\Bbbk$-algebra. The *Hankel operator* of $\phi \in \mathsf{Hom}(\mathcal{A}, \Bbbk)$ is

$$H_\phi : \mathcal{A} \to \mathsf{Hom}(\mathcal{A}, \Bbbk), \quad p \mapsto p \star \phi.$$

Similarly, if $\mathcal{A} = \oplus_{i=0}^{\infty} \mathcal{A}_i$ is graded, for every $\phi \in \mathsf{Hom}(\mathcal{A}_d, \Bbbk)$ and $c \leq d$ we define its *restriction in degree* $(d-c, c)$ as $H_\phi^{d-c,c} : \mathcal{A}_c \to \mathsf{Hom}(\mathcal{A}_{d-c}, \Bbbk),\ p \mapsto p \star \phi$. Finally, if V, W are $\Bbbk$-vector spaces such that $V \cdot W \subseteq \mathcal{A}_d$, we define the *truncated Hankel operator* $H_\varphi^{W,V} : V \to \mathsf{Hom}(W, \Bbbk),\ p \mapsto (p \star \varphi)^{[W]}$ by restricting the (co)domain of H_φ.

We can now state our main result, which relates I_φ to the Hankel operator of

$$\check{f} : \Bbbk[x_1, \ldots, x_n]_{\leq d} \to \Bbbk, \quad g \mapsto f^*\big(\mathfrak{h}_0(g)\big),$$

where $\mathfrak{h}_0(g)$ is the homogenization of g in degree-d, with respect to the variable x_0.

We will consider the quotient algebra $\mathcal{A}_\varphi = \Bbbk[x_0, \ldots, x_n]/I_\varphi$, and its dehomogenization $\mathcal{A} = \Bbbk[x_1, \ldots, x_n]/I$ obtained as the image of the projection $x_0 \mapsto 1, x_i \mapsto x_i\ \forall\, 1 \leq i \leq n$.

Theorem 3. *Let $c \leq d$ and B, B' be $\Bbbk$-bases of $\mathcal{A}$ such that $1 \in B$, $x_i B \subset \Bbbk[x_1, \ldots, x_n]_{\leq c}$ for every $1 \leq i \leq n$, and $B' \subset \Bbbk[x_1, \ldots, x_n]_{\leq d-c}$. Then we have the following:*

1. *$H_0 := H_{\check{f}}^{\langle B' \rangle, \langle B \rangle}$ is invertible.*
2. *$\operatorname{rank} H_{\check{f}}^{d-c,c} = \dim \mathcal{A} = \sum_{i=1}^{s} \dim \langle\langle \omega_i^{d, \ell_i, (x_1, \ldots, x_n)} \rangle\rangle$.*
3. *For every $1 \leq i \leq n$, let $H_i = H_{\check{f}}^{\langle B' \rangle, \langle x_i B \rangle}$. Then $M_{x_i} = H_0^{-1} H_i$ is the matrix of the multiplication-by-x_i operator on $\mathcal{A}$, with respect to the basis B.*
4. *$\ker H_{\check{f}}^{d-c,c} = I_{\leq c}$ and $(\ker H_{\check{f}}^{d-c,c}) = I$.*

The assumptions of Theorem 3 are satisfied when $\mathcal{A}$ is generated in degree lower than $\min\{d-c, c-1\}$. In such cases, if $\Bbbk = \overline{\Bbbk}$, one can compute the ℓ_i's by using part (3) of Theorem 3, together with the following result. Over general fields (e.g., $\Bbbk = \mathbb{R}$), it provides a lower bound for the GAD-rank over $\Bbbk$, with equality when a minimal GAD is $\Bbbk$-rational.

Proposition 4. *Let $\mathcal{A} = \bigoplus_{k=1}^{s} \mathcal{A}_{\xi_k}$ be an Artinian algebra, with $\mathcal{A}_{\xi_k}$ local and supported at $\xi_k \in \Bbbk^n$. Let $\lambda \in \Bbbk[x_1, \ldots, x_n]_1$ be a generic linear form, and $M_\lambda = U T U^{-1}$ be the Schur factorization of the multiplication-by-λ operator on $\mathcal{A}$. Then, for any $g \in \Bbbk[x_1, \ldots, x_n]$, the conjugated multiplication operator $\tilde{M}_g := U^{-1} M_g U$ is block upper triangular, i.e.,*

$$\tilde{M}_g = \begin{bmatrix} \tilde{M}_g^{(1)} & * & \cdots & * \\ 0 & \tilde{M}_g^{(2)} & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \tilde{M}_g^{(s)} \end{bmatrix},$$

where each block $\tilde{M}_g^{(k)}$ represents the multiplication-by-g in $\mathcal{A}_{\xi_k}$. Moreover, the eigenvalues of M_λ are the evaluation of λ at the supports ξ_k, with algebraic multiplicity $\dim \mathcal{A}_{\xi_k}$.

Proposition 4 allows us to compute the supports ℓ_i and the local weights of a GAD from the blocks $\{\tilde{M}_{x_j}^{(i)}\}_{1 \leq i \leq s, 1 \leq j \leq n}$. We can also recover the k_i's from the following result.

Proposition 5. *Let I be the affine ideal associated with a GAD, and the $M_{x_j}^{(i)}$ be the blocks of the multiplication-by-x_j matrices on $\mathbb{k}[x_1,\dots,x_n]/I$, as above. Then*

$$k_i = \min_{N\in\mathbb{N}} \left\{ \left(M_{x_j}^{(i)}\right)^N = 0 \,\forall\, 1 \le j \le n \right\} - 1.$$

Identifiability of minimal GADs

Theorem 3 yields a criterion for the uniqueness of minimal GADs, which depends on the Castelnuovo–Mumford regularity $\operatorname{reg}\mathbb{k}[x_1,\dots,x_n]/I_\varphi$ of the associated scheme.

Theorem 6. *Let $1 \le c \le d$ and I_φ be the ideal associated to a GAD of $f \in \mathbb{k}[x_0,\dots,x_n]_d$. If $\operatorname{reg}\mathbb{k}[x_0,\dots,x_n]/I_\varphi \le \min\{d-c, c-1\}$, then*

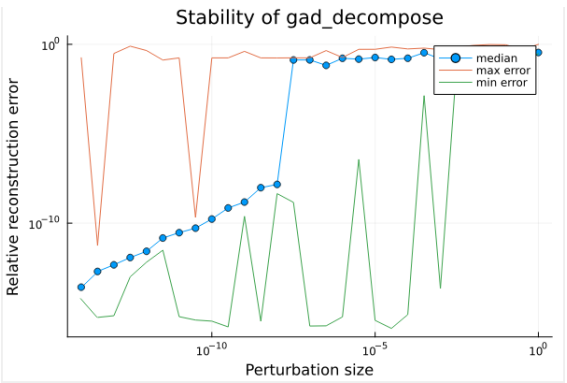
$$\mathrm{rk}_{\mathsf{GAD}}(f) = \mathrm{rk} H_{f^*}^{d-c,c},$$

and the considered GAD is the unique minimal one, up to permutation of the terms.

Conclusion and numerical testing

The presented method advances previous eigenvalue approaches [5], and our Julia implementation [10] demonstrates numerical stability and robustness under small perturbations. As an instance, let us consider the symmetric tensor $f = (x_0+x_2)^4(x_0+x_1) - 2x_0^3(x_0x_1 + x_1^2)$.

$$\tilde{M}_{x_1} = \left[\begin{array}{ccc|cc} \mathbf{0} & \frac{1}{7} & 0 & 0 & 0 \\ 0 & \mathbf{0} & \frac{1}{7} & 0 & 0 \\ 0 & 0 & \mathbf{0} & 0 & 0 \\ \hline 0 & 0 & 0 & \mathbf{0} & \frac{1}{18} \\ 0 & 0 & 0 & 0 & \mathbf{0} \end{array}\right] \qquad \tilde{M}_{x_2} = \left[\begin{array}{ccc|cc} \mathbf{0} & 0 & 0 & 0 & 0 \\ 0 & \mathbf{0} & 0 & 0 & 0 \\ 0 & 0 & \mathbf{0} & 0 & 0 \\ \hline 0 & 0 & 0 & \mathbf{1} & -\frac{1}{18} \\ 0 & 0 & 0 & 0 & \mathbf{1} \end{array}\right]$$



By Theorem 3, the multiplication matrices M_{x_1}, M_{x_2} can be constructed from $H_{\tilde{f}}^{2,3}$. By Proposition 4, we read the supports $\ell_1 = x_0 + 0\cdot x_1 + 0\cdot x_2$ and $\ell_2 = x_0 + 0\cdot x_1 + 1\cdot x_2$ from the traces of their simultaneous Jordan forms $\tilde{M}_{x_1}, \tilde{M}_{x_2}$, while we compute $k_1 = 2, k_2 = 1$ from the nilpotencies of their Jordan blocks, by Proposition 5. Finally, we recover the above

GAD of f by solving a linear system. The Hilbert series of I_φ is $(1, 3, 5, 5, \dots)$, therefore $\operatorname{reg} \Bbbk[x_0, \dots, x_n]/I_\varphi = 2 \leq \min\{5-3, 3-1\}$, so this is the unique minimal GAD of f by Theorem 6. The above chart displays the numerical stability of this method [10].

Acknowledgements. The first author has been supported by European Union's HORIZON–MSCA-2023-DN-JD programme under the Horizon Europe (HORIZON) Marie Sklodowska-Curie Actions, grant agreement 101120296 (TENORS). The last author has been supported by Research Foundation - Flanders (FWO: 12ZZC23N), and by the BOF project C16/21/002 by the Internal Funds of KU Leuven.

References

[1] J. Alexander, A. Hirschowitz: Polynomial interpolation in several variables. *J. Algebraic Geom.* **4**, 201–222 (1995).

[2] E. Barrilli, B. Mourrain, D. Taufer: Generalized Additive Decompositions of Symmetric Tensors. *ArXiv:2510.25681* (2025).

[3] A. Bernardi, J. Jelisiejew, P.M. Marques, K. Ranestad: On polynomials with given Hilbert function and applications. *Collect. Math.* **69**, 39–64 (2018).

[4] A. Bernardi, A. Oneto, D. Taufer: On schemes evinced by generalized additive decompositions and their regularity. *J. Math. Pures Appl.* **188**, 446–469 (2024).

[5] A. Bernardi, D. Taufer: Waring, tangential and cactus decompositions. *J. Math. Pures Appl.* **143**, 1–30 (2020).

[6] A. Iarrobino, V. Kanev: *Power sums, Gorenstein algebras, and determinantal loci*. Lecture Notes in Mathematics **1721**, Springer Berlin Heidelberg (1999).

[7] J.M. Landsberg: *Tensors: Geometry and Applications*. Graduate Studies in Mathematics **128**, American Mathematical Society (2012).

[8] B. Mourrain: Polynomial–Exponential Decomposition From Moments. *Found. Comput. Math.* **18**, 1435–1492 (2017).

[9] O. Reig Fité, D. Taufer: Determinantal computation of minimal local GADs. *ArXiv:2603.08836* (2026).

[10] Numerical implementation (Julia): `https://github.com/enricabarrilli/GAD.jl`

Computing the characteristic polynomial of linearized polynomials via Drinfeld Modules

L. Bastioni[◇*], G. Micheli[*], S. Zhao[*]

[◇] *Speaker at EACA 2026*

[*] *University of South Florida*

lbastioni@usf.edu, gmicheli@usf.edu, shujunz@usf.edu

Abstract. Let k be a finite field, and L be a q-linearized polynomial defined over k of q-degree r, namely $L = \sum_{i=0}^{r} a_i Z^{q^i}$, with $a_i \in k$. This work provides an algorithm to compute the characteristic polynomial of L over a large extension field $\mathbb{F}_{q^n} \supseteq k$. Our algorithm has computational complexity of $O(n(\log(n))^4)$ in terms of $\mathbb{F}_q$ operations with the implied constant depending only on k and r. Up to logarithmic factors, and for linear maps represented by low degree polynomials, such algorithm provides a square root improvement over the state of art.

Introduction

Characteristic polynomial of a matrix

Let $A \in \mathrm{Mat}_n(K)$, where K is a field. Computing the characteristic polynomial of A is a classical problem. In 1985, Keller-Gehrig [7] reduced this problem to a matrix multiplication problem, obtaining an algorithm with complexity $O(n^\omega \log(n))$ in general, and $O(n^\omega)$ when A is generic matrix: each of whose coefficients can be considered as an independent indeterminate. Here, ω denotes the exponent of the optimal time complexity of matrix multiplication, for which it's known that $2 \leq \omega \leq 3$, with the current best bound being $\omega < 2.371866$ [4]. In 2007, C. Pernet and A. Storjohann [11] showed that the characteristic polynomial can be computed with expected cost $O(n^\omega)$, improving by a factor of $\log(n)$ Keller-Gehrig's bound, with a success probability of at least 1/2, provided the field F contains at least $2n^2$ elements. More recently, in 2021, V. Neiger and C. Pernet [9] removed both the randomness and field size restriction, presenting a deterministic algorithm that achieves complexity $O(n^\omega)$ for computing the characteristic polynomial of any matrix over an arbitrary field K.

Characteristic polynomial of endomorphisms of Drinfeld modules

Let $A = \mathbb{F}_q[T]$ be the ring of polynomials. Let ϕ be a Drinfeld module of rank r over $k = \mathbb{F}_{q^n}$ with A-characteristic $\mathfrak{p}$ of degree d. In [8], the authors Y. Musleh and É. Schost developed an algorithm to compute the characteristic polynomial of an arbitrary endomor-

J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, V. Sotomayor (eds.): Proceedings of the XIX EACA, pp. 60-64 (2026).
ISBN: 978-84-09-87277-0

phism $u \in \mathrm{End}_k(\phi)$ of a finite Drinfeld module using its associated crystalline cohomology. The algorithm is faster when $u = \tau^n$ is the Frobenius endomorphism and $d = n$. In this case, the algorithm attains a bit complexity of $(r^\omega n^{1.5} \log q + n \log^2 q)^{1+o(1)}$, where ω is the exponent of the optimal time complexity of matrix multiplication as mentioned before. For $u = \tau^n$ and $d < n$, the characteristic polynomial could be computed with bit complexity $(r^\lambda/d + r^\omega/\sqrt{d})n^2 \log q + n \log^2 q)^{1+o(1)}$, where λ denotes an exponent such that the characteristic polynomial of an $s \times s$ matrix over a ring R can be computed in $O(s^\lambda)$. When R is a field this can be done with the same cost of matrix multiplication and so $\lambda = \omega$. For general rings, the best known value as of today is $\lambda \approx 2.7$ (see [6]). When r and q is fixed, the first complexity is essentially linear in $n^{1.5}$, and the second one is linear in n^2. Another important contribution is due to X. Caruso and A. Leudière [3], who proposed several algorithms to compute characteristic polynomials of endomorphisms of Drinfeld modules. Among these, their most efficient algorithm is for computing the characteristic polynomial of the Frobenius and achieves a cost of $O((n^2 r + nr^\omega) \log q)$ operations in k.

A square root improvement to the computation of the characteristic polynomial of a low degree linearized polynomial

Let k be a finite field, and L be a q-linearized polynomial defined over k of q-degree r ($L = \sum_{i=0}^{r} a_i Z^{q^i}$, with $a_i \in k$). In this work we provide an algorithm to compute the characteristic polynomial of L over a large extension field $\mathbb{F}_{q^n} \supseteq k$. Our algorithm, that relies on the use of the characteristic polynomial of the Frobenius endomorphism of a Drinfeld Module, has computational complexity of $O(n(\log(n))^4)$ in terms of $\mathbb{F}_q$ operations, and with the implied constant depending only on k and r. This is essentially better than a square root improvement (up to logarithmic factors) of the state of art: as mentioned before, if one were to compute the characteristic polynomial of L as an $\mathbb{F}_q$-linear map over $\mathbb{F}_{q^n}$ one would have a complexity of $O(n^\omega)$, where $\omega \in [2, 3]$. In other words, in this work we show that if a linear map comes from a q-polynomial of low degree, then the computation of its characteristic polynomial is much faster than the one of linear maps having a large degree q-polynomial representing it (in fact, it is an easy exercise to show that all linear maps over finite fields can be represented by linearized polynomials).

Main results

Complete proofs of the results stated in this section are provided in [2].

Let $m > 0$ be an integer, p a prime number, q a p-power, and $\mathbb{F}_{q^m}$ the finite field with q^m elements. Let $0 < \ell \in \mathbb{N}$ be a positive integer and consider now the Drinfeld module attached to $L = \sum_{i=0}^{r} t_i Z^{q^i} \in \mathbb{F}_{q^m}[Z]$ over the extension $k' = \mathbb{F}_{q^{m\ell}}$ defined by

$$\phi^{(\ell)} : \mathbb{F}_q[T] \to k'\{\tau\}$$
$$T \mapsto \phi_T^{(\ell)} = \sum_{i=0}^{r} t_i \tau^i.$$

We suppose that $t_0 \in \mathbb{F}_{q^d}$ for a $d|m$, and $\mathbb{F}_q(t_0) = \mathbb{F}_{q^d}$. Since $\gamma(T) = t_0$, then the $\mathbb{F}_q[T]$-characteristic of k' is $\mathfrak{p} = (m_{t_0})$ where m_{t_0} is the minimal polynomial of t_0 over $\mathbb{F}_q$. Let $\pi = \tau^{m\ell}$ be the Frobenius for k', let $P_{\phi^{(\ell)}} := P_{\phi^{(\ell)}}(X)$ be the characteristic polynomial of π when acting on the $\mathfrak{l}$-adic Tate module $T_{\mathfrak{l}}(\phi^{(\ell)})$ of $\phi^{(\ell)}$. From [10, Theorem 4.2.2] we know that $P_{\phi^{(\ell)}}$ has coefficients in $\mathbb{F}_q[T]$ which do not depend on the choice of the prime $\mathfrak{l} \in \mathbb{F}_q[T]$.

For a polynomial $F \in K[X]$, let $F = \prod_{i=1}^{\deg(F)}(X - \alpha_i)$ be its factorization into linear factors (with possible repeated roots) in $\bar{K}[X]$, where $\bar{K}$ is the algebraic closure of K. Let $\varepsilon_\ell : K[X] \to \bar{K}[X]$ be the map defined by $\varepsilon_\ell(F) = \prod_{i=1}^{\deg(F)}(X - \alpha_i^\ell)$. We have then the following result.

Proposition 1. ([2, Corollary 3.5]) $P_{\phi^{(\ell)}} = \varepsilon_\ell(P_{\phi^{(1)}})$.

From now on, let's denote by $C_L^{(\ell)} \in \mathbb{F}_q[T]$ the characteristic polynomial of $L \in \mathbb{F}_{q^m}[Z]$ seen as a linear map over $k' = \mathbb{F}_{q^{m\ell}}$.

In general, if ϕ is a Drinfeld module defined over an $\mathbb{F}_q[T]$-field k, let ${}^\phi k$ denote the $\mathbb{F}_q[T]$-module, whose underlying group is $(k, +)$ subject to the action defined by $a \circ \beta := \phi_a(\beta)$ for every $a \in \mathbb{F}_q[T]$ and $\beta \in k$. Since ${}^\phi k$ is finitely generated, then we have an isomorphism

$$ {}^\phi k \cong \mathbb{F}_q[T]/(a_1) \oplus \ldots \oplus \mathbb{F}_q[T]/(a_s) $$

for uniquely determined monic polynomials $a_1, \ldots, a_s \in \mathbb{F}_q[T]$ of positive degrees such that $a_i \mid a_{i+1}$. Each a_i is called an *invariant factor* of ${}^\phi k$, and the product of all the invariant factors $\chi({}^\phi k) := \prod_{i=1}^s a_i$ is called the *fitting ideal* of ${}^\phi k$. As a standard linear algebra fact (see for example [10, Exercise 1.2.7] or [5, Chapter 12, Proposition 20]), we also know that $\chi({}^\phi k)$ is the characteristic polynomial of ϕ_T considered as an $\mathbb{F}_q$-linear map over k. This means that, setting $\phi = \phi^{(\ell)}$ and $k = k'$, we have $\chi({}^\phi k) = C_L^{(\ell)}$. Finally, as a consequence of [10, Theorem 4.2.6], observe that $(P_{\phi^{(\ell)}}(1)) = (\chi({}^\phi k)) = (C_L^{(\ell)})$ which implies, using Proposition 1, that $C_L^{(\ell)} = v^{(\ell)} P_{\phi^{(\ell)}}(1) = v^{(\ell)} \varepsilon_\ell(P_{\phi^{(1)}})(1)$ for some $v^{(\ell)} \in \mathbb{F}_q$.

Proposition 2. ([2, Corollary 4.11]) Let $L \in \mathbb{F}_{q^m}[Z]$ be a linearized polynomial of q-degree r. Then the sequence $\{C_L^{(\ell)}\}_{\ell \in \mathbb{N}_{>0}} \subseteq \mathbb{F}_q[T]$ of characteristic polynomials of L as a linear map on $\mathbb{F}_{q^{m\ell}}$ is a linear recurrence sequence of order at most 2^r.

Proposition 3. ([2, Proposition 4.13]) *There exists a characteristic polynomial of degree at most 2^r for the sequence $\{C_L^{(\ell)}\}_{\ell \in \mathbb{N}_{>0}} \subseteq \mathbb{F}_q[T]$ with coefficients having T-degrees upper bounded by $m2^{r-1}$. In particular, such bound does not depend on q or ℓ.*

The algorithm

We refer the reader to [2] for completeness.

Write a linear recurrence relation for $\{C_L^{(\ell)}\}_{\ell \in \mathbb{N}_{>0}}$ of order $d \leq 2^r$ as:

$$ C_L^{(k+d)} = c_{d-1} C_L^{(k+d-1)} + \ldots + c_1 C_L^{(k+1)} + c_0 C_L^{(k)}, \tag{1} $$

where $c_i \in \mathbb{F}_q[T]$. Suppose also that for $i = 0, \ldots, d-1$ we have $\deg c_i \leq B$, where B does not depend on q or ℓ. Let now $\ell > 2^{r+1}$ and $n = m\ell$.

Step 1: Initialization of the algorithm (independent of ℓ)

For $i = 1, \ldots, 2^{r+1}$, compute $C_L^{(i)}$. Using standard algorithms already known in literature (see for example [7], [11],[9]), each characteristic polynomial can be computed in at most $O((mi)^\omega \log(mi))$ operations over $\mathbb{F}_q$, where it is $\omega \in (2, 3]$. This means that such initialization totally costs at most $O(m^\omega (2^{r+1})^{\omega+1} \log(2md))$ operations over $\mathbb{F}_q$.

Step 2: Compute the coefficients of the recursion (independent of ℓ)

Compute coefficients $c_0, \ldots, c_{d-1} \in \mathbb{F}_q[T]$ of the characteristic polynomial of the linear recurrence relation (1). It is sufficient to solve the following system of linear equations:

$$\{C_L^{(i+d)} = c_{d-1} C_L^{(i+d-1)} + \ldots + c_1 C_L^{(i+1)} + c_0 C_L^{(i)}\}_{i=1,\ldots,d},$$

for $c_0, \ldots, c_{d-1}$. This system can be solved using Gaussian elimination with a computational complexity of at most $O(d^3)$ operations over $\mathbb{F}_q[T]$.

Step 3: Compute linear recursion for evaluations of the sequence

In this step we compute evaluation points and their values to recover $C_L^{(\ell)}$ by interpolation at the next step.

Case 1. Suppose $q > n$ so that we have enough space to choose n evaluation points $x_1, \ldots, x_n$ in $\mathbb{F}_q$. Computing all the evaluations costs at most $O((md^2 + Bd)n + d^3 n \log(n))$ multiplications over $\mathbb{F}_q$.

Case 2. Suppose $q < n$. Then, in order to have enough evaluation points, we need to enlarge the base field. It is sufficient to choose points over $\mathbb{F}_{q^{\lceil \log_q(n) \rceil}}$. We have that to compute all the evaluations costs at most $O((md^2 + Bd)n \log^2(n) + d^3 n \log^3(n))$ multiplications over $\mathbb{F}_q$.

Step 4: Interpolation

Construct $C_L^{(\ell)}$ by interpolation.

Case 1. Suppose $q > n$. Then interpolation can be done using $O(n \log^2(n))$ arithmetic operations over $\mathbb{F}_q$ (see for example [1, Theorem 8.14]).

Case 2. If $q < n$, then interpolation must be performed over an extension field of $\mathbb{F}_q$. The smallest such extension is $\mathbb{F}_{q^{\lceil \log_q n \rceil}}$, where each multiplication corresponds to $\log_q^2 n \approx \log^2(n)$ multiplications in $\mathbb{F}_q$. This means that such interpolation needs $O(n \log^4(n))$ operations over $\mathbb{F}_q$.

Acknowledgements. This work was supported by the National Science Foundation under Grant No 2338424.

References

[1] A.V. Aho, J.E. Hopcroft: *The Design and Analysis of Computer Algorithms*. Addison-Wesley Longman, 1st edition (1974).

[2] L. Bastioni, G. Micheli, S. Zhao: On the Characteristic Polynomial of Linearized Polynomials. *ArXiv:2506.16937v1* (2025).

[3] X. Caruso, A. Leudière: Algorithms for computing norms and characteristic polynomials on general drinfeld modules. *Math. Comp.* **95**, 415–455 (2026).

[4] R. Duan, H. Wu, R. Zhou: Faster matrix multiplication via asymmetric hashing. *2023 IEEE 64th Annual Symposium on Foundations of Computer Science (FOCS)*, 2129–2138 (2023).

[5] D.S. Dummit, R.M. Foote: *Abstract algebra*. Wiley (2004).

[6] E. Kaltofen, G. Villard: On the complexity of computing determinants. *Comput. Complex.* **13**(3), 91–130 (2005).

[7] W. Keller-Gehrig: Fast algorithms for the characteristics polynomial. *Theoret. Comput. Sci.* **36**, 309–317 (1985).

[8] Y. Musleh, É. Schost: Computing the characteristic polynomial of endomorphisms of a finite drinfeld module using crystalline cohomology. *Proc. ISSAC 2023*, 461–469 (2023).

[9] V. Neiger, C. Pernet: Deterministic computation of the characteristic polynomial in the time of matrix multiplication. *J. Complexity* **67**, 101572 (2021).

[10] M. Papikian: *Drinfeld Modules*. Springer (2023).

[11] C. Pernet, A. Storjohann: Faster algorithms for the characteristic polynomial. *Proc. ISSAC 2007*, 307–314. ACM (2007).

Extension of root-based attacks against PLWE for the fully-split case

I. Blanco-Chacón*, R. Durán Díaz*, R. Martín Sánchez-Ledesma◇†

◇ *Speaker at EACA 2026*

* *Universidad de Alcalá*

† *Universidad Complutense de Madrid, and Indra Sistemas de Comunicaciones Seguras*

ivan.blancoc@uah.es, raul.duran@uah.es, rodrma01@ucm.es / rmsanchezledesma@indra.es

Abstract. In the present work, we study an extension to the attacks in [1] via the construction of explicit isomorphisms from vulnerable instances, and provide a formal proof that this approach will not yield any new vulnerabilities under a fully-split setting.

Introduction

An important debate in cryptography in general, and post-quantum cryptography in particular, is the one contrasting efficiency with security. For lattice-based cryptography, this dilemma is represented via unstructured and structured lattice schemes [4]. The question is then: *Are structured lattices vulnerable to attacks beyond those applied to general lattices?*

It is precisely this line of thought that the works of [2, 3] analyze. In them, a general framework is introduced to exploit the algebraic structure of *Polynomial Learning With Errors* schemes, one of the most important paradigms in PQC, in order to construct *decisional* attacks. These attacks have been later expanded and generalized in [1].

The present work intends to answer another question that remains still open: *Can the attacks be transferred to a vulnerable setting, from where some information might be inferred?*.

This work proves precisely that it cannot be done, under the application of isomorphisms in a fully-split setting: we will show that no isomorphism between fully-split PLWE instances provides any meaningful advantage over attacking the original PLWE instance.

Preliminaries

Definition 1 (PLWE distribution)**.** Let q be a rational prime, $f(x) \in \mathbb{Z}[x]$ a monic irreducible polynomial in $\mathbb{Z}[x]$, and $\mathcal{O}_f$ the associated quotient ring $\mathbb{Z}[x]/(f(x))$. Let χ be a discrete random distribution with values in $\mathcal{O}_f/q\mathcal{O}_f$. For $s \in \mathcal{O}_f/q\mathcal{O}_f$, we define the *PLWE distribution* $\mathcal{B}_{s,\chi}$ as the distribution over $\mathcal{O}_f/q\mathcal{O}_f \times \mathcal{O}_f/q\mathcal{O}_f$ obtained by sampling an element a in

J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, V. Sotomayor (eds.): Proceedings of the XIX EACA, pp. 65-69 (2026).
ISBN: 978-84-09-87277-0

$\mathcal{O}_f/q\mathcal{O}_f$ uniformly at random, drawing an element e according to χ, and returning the pair $(a, a \cdot s + e) \in (\mathcal{O}_f/q\mathcal{O}_f \times \mathcal{O}_f/q\mathcal{O}_f)$.

Let $\mathcal{G}$ be a Gaussian distribution of mean 0 and variance σ^2. With $f(x)$, q and σ, we have our (f, q, σ)-PLWE instance.

Definition 2. Two N-degree separable polynomials, $f(x)$ and $g(x)$ are said to have the same *factorization structure* in $\mathbb{F}_q[x]$ if their factorizations, $f(x) = \prod_{i=1}^{\ell_1} f_i(x)$, and $g(x) = \prod_{i=1}^{\ell_2} g_i(x)$, with each $f_i(x), g_i(x)$ irreducible in $\mathbb{F}_q[x]$, are such that $\ell_1 = \ell_2 = \ell$, and there exists a bijection between $i \in \{1, \ldots, \ell\}$ and $j \in \{1, \ldots, \ell\}$ such that $f_i(x)$ and $g_j(x)$ have the same degree.

Proposition 3. *Let $f(x), g(x) \in \mathbb{Z}[x]$ be monic polynomials of degree N irreducible in $\mathbb{Z}[x]$ having the same* factorization structure *in $\mathbb{F}_q[x]$. Then, there exists an isomorphism between the rings $R_q := \mathbb{F}_q[x]/(f(x))$ and $R'_q := \mathbb{F}_q[x]/(g(x))$.*

Extension via isomorphisms of rings

Let $g(x)$ be also a monic polynomial of degree N irreducible in $\mathbb{Z}[x]$ that has an n-ideal factor in $\mathbb{F}_q$ having the same *factorization structure* as $f(x)$.

The idea of the extension via isomorphisms is as follows:

- To begin with, every (f, q, σ)-PLWE sample is transformed into a (g, q, σ)-PLWE sample via the existing isomorphism between R_q and R'_q by virtue of Proposition 3. This transformation retains the behavior of both PLWE and uniform samples.
- Then, we use the homomorphism derived from the evaluation at root α of the n-ideal factor $x^n - a$ of $g(x)$ to migrate our samples into $\mathbb{F}_{q^n}$.
- From that point on, we are entitled to apply any of the attacks in [1] to $\mathbb{F}_{q^n}$, in order to create a successful decisional attack.

Suppose now that both $f(x)$ and $g(x)$ decompose into linear factors over $\mathbb{F}_q$ and the roots, $(\alpha_1, \ldots, \alpha_N)$, $(\beta_1, \ldots, \beta_N)$, respectively, are distinct. Then, we are able to construct an explicit isomorphism between R_q and R'_q.

- The isomorphism ϕ_1, derived from the Chinese Remainder Theorem,
$$\phi_1 \colon R_q \to \prod^{N} \mathbb{F}_q.$$
- The inverse isomorphism, ϕ_2^{-1} derived also from the Chinese Remainder Theorem,
$$\phi_2 \colon R'_q \to \prod^{N} \mathbb{F}_q.$$

Given $a(x) \in R_q$, then $\phi_1(a(x)) = (a(\alpha_1), \ldots, a(\alpha_N))$ that can be naturally described by means of the Vandermonde matrix of the roots of $f(x)$ in $\mathbb{F}_q$: Defining the vector $\mathbf{a} =$

$(a_0, \ldots, a_{N-1})$, we have $\phi_1(a(x)) = V_f \cdot \mathbf{a}$, where

$$V_f = \begin{bmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{N-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_N & \cdots & \alpha_N^{N-1} \end{bmatrix},$$

and, analogously, V_g for the Vandermonde matrix of the roots of $g(x)$.

Note that different isomorphisms can be constructed from the permutation of the order of the roots, which just consists of a permutation transformation P_σ.

We choose, in general, any root ξ. If we denote the isomorphism matrix as $M := V_g^{-1} \cdot V_f$, as given by

$$M = \begin{bmatrix} 1 & x_{1,2} & \cdots & x_{1,N} \\ 0 & x_{2,2} & \cdots & x_{2,N} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & x_{N,2} & \cdots & x_{N,N} \end{bmatrix},$$

then we can write the transformation in matrix notation as $\mathbf{b} = M \cdot \mathbf{a}$, namely,

$$\begin{aligned} b_0 &= a_0 + \sum_{j=1}^{N-1} x_{1,j+1} \cdot a_j, \\ b_i &= \sum_{j=1}^{N-1} x_{i,j+1} \cdot a_j, \qquad 2 \leq i \leq N, \end{aligned}$$

so that the transformed sample in polynomial representation becomes

$$b(y) = a_0 + \sum_{i=1}^{N} y^{i-1} \sum_{j=1}^{N-1} x_{i,j+1} \cdot a_j. \tag{1}$$

In the general case, following Equation (1), we end up with evaluation terms of the form

$$b(\xi) = a_0 + \sum_{i=1}^{N} \xi^{i-1} \sum_{j=1}^{N-1} x_{i,j+1} \cdot a_j = a_0 + \sum_{j=1}^{N-1} a_j \cdot S_{j+1,\xi}(M),$$

where $S_{j,\xi}(M) = \sum_{i=1}^{N} \xi^{i-1} \cdot x_{i,j}$ is precisely the sum of all the entries in the j-th column of the matrix M, weighted by the powers of the root ξ.

Each of the entries of the isomorphism matrix can be represented as

$$x_{i,j} = \sum_{k=1}^{N} (-1)^{i+k} \frac{\alpha_k^{j-1}}{Q_k(\beta_1, \ldots, \beta_N)} E_{N-i,k}(\beta_1, \ldots, \beta_N),$$

with $Q_j(\xi_1, \ldots, \xi_n)$ defined as

$$Q_j(\xi_1, \ldots, \xi_n) := \prod_{l=1}^{j-1} (\xi_j - \xi_l) \cdot \prod_{l=j+1}^{n} (\xi_l - \xi_j).$$

and $E_{j,k}(X_1, \ldots, X_n)$ defined as

$$E_{j,k}(X_1, \ldots, X_n) := E_j(X_1, \ldots, X_{k-1}, X_{k+1}, \ldots, X_n).$$

Thus, the sum $S_{j,\xi}(M)$ can be expressed as

$$\begin{aligned} S_{j,\xi}(M) &= \sum_{i=1}^{N} \xi^{i-1} \sum_{k=1}^{N} (-1)^{i+k} \frac{\alpha_k^{j-1}}{Q_k(\beta_1, \ldots, \beta_N)} E_{N-i,k}(\beta_1, \ldots, \beta_N) \\ &= \sum_{k=1}^{N} \frac{\alpha_k^{j-1}}{Q_k(\beta_1, \ldots, \beta_N)} \sum_{i=1}^{N} (-1)^{i+k} \xi^{i-1} E_{N-i,k}(\beta_1, \ldots, \beta_N). \end{aligned}$$

After a number of computations regarding symmetric elemental polynomials, we realize that

$$S_{j,\beta_\ell}(M) = (-1)^{N+\ell} \frac{\alpha_\ell^{j-1}}{Q_\ell(\beta_1, \ldots, \beta_N)} G_\ell(\beta_\ell; \beta_1, \ldots, \beta_N) = \alpha_\ell^{j-1}.$$

where $G_k(\lambda; X_1, \ldots, X_n) := \prod_{i=1, i\neq k}^{n} (\lambda - X_i)$.

Therefore, for any arbitrary root of $g(x)$, β_ℓ, we get the general evaluated term

$$b(\beta_\ell) = \sum_{j=0}^{N-1} a_j \cdot \alpha_\ell^j.$$

We can claim then that the evaluated samples will not be subject to any of the attacks, since the evaluation is given in terms of the roots of the polynomial $g(x)$ is not subject to attacks. Thus, we have proven that fully-split polynomials are secure, even in the face of constructing these isomorphisms to other *vulnerable* settings.

The above realization, combined with the following theorem, shows that root-based attacks cannot be extended via isomorphisms of ring to produce more easily attackable instances.

Theorem 4. *Let q be a prime and $f(x), g(x)$ be irreducible polynomials over $\mathbb{Z}[x]$ such that they factor completely over $\mathbb{F}_q[x]$ with $\{\alpha_i\}_{i=1}^N$ the set of roots of $f(x)$ in $\mathbb{F}_q[x]$, and $\{\beta_i\}_{i=1}^N$ the set of roots of $g(x)$ in $\mathbb{F}_q[x]$. Then, any ring isomorphism*

$$\psi \colon \mathbb{F}_q[x] / \prod_{i=1}^{N} (x - \alpha_i) \to \mathbb{F}_q[x] / \prod_{i=1}^{N} (x - \beta_i)$$

is of the form $V_g^{-1} \cdot V_f$, where V_f, V_g represent the Vandermonde matrices of the roots of the (fully-split) polynomials $f(x)$ and $g(x)$ over $\mathbb{F}_q[x]$.

Acknowledgements. The first author is partially supported by the Spanish National Research Plan, grant PID2022-136944NB-I00, by grant PID2019-104855RB-I00, funded by MCIN/AEI/10.13039/501100011033 and, along with R. Durán Díaz, by the Universidad de Alcalá grant CCG20/IA-057. The third author is partially supported by the PQReact Project. This project has received funding from the European Union's Horizon Europe research and innovation program under grant agreement no. 10111954.

References

[1] I. Blanco Chacón, R. Durán Díaz, R. Martín Sánchez-Ledesma: A generalized approach to root-based attacks against PLWE. *Cryptogr. Commun.* 1–45 (2025).

[2] Y. Elias, K.E. Lauter, E. Ozman, K.E. Stange: *Probably weak instances of ring-LWE*. Advances in Cryptology – CRYPTO 2015, Lecture Notes in Computer Science. Springer (2015).

[3] Y. Elias, K.E. Lauter, E. Ozman, K.E. Stange: *Ring-LWE cryptography for the number theorist*. Directions in Number Theory, Association for Women in Mathematics Series. Springer (2016).

[4] V. Lyubashevsky, C. Peikert, O. Regev: On ideal lattices and learning with errors over rings. *J. ACM* **60**(6), 1–35 (2013).

MacWilliams duality for rank metric codes over finite chain rings

I. Blanco Chacón*, A.F. Boix†, V. García Benítez◇†

◇ *Speaker at EACA 2026*

* *Department of Mathematics, Schools of Science, Universidad de Alcalá de Henares*

† *Department of Mathematics, Universitat Politècnica de Catalunya, BarcelonaTech*

ivan.blancoc@uah.es, alberto.fernandez.boix@upc.edu, victoria.garcia.benitez@upc.edu

Abstract. The goal of this report is to present an extension of Ravagnani's MacWilliams duality theory to the setting of rank metric codes over finite chain rings, relating the sequences of q-binomial moments of a rank metric code over this class of rings with those of its dual.

Introduction

MacWilliams identities relate the weight distribution of a code to that of its dual. Originally established for linear codes over finite fields with the Hamming metric [6], they were later generalized to non-linear codes under the complete and Lee metrics [7].

Further on, Delsarte introduced rank-metric codes in [2]. These codes are linear subspaces of matrices over finite fields, where the distance between two matrices is defined as the rank of their difference. Delsarte's approach interprets rank-metric codes as association schemes, for which the MacWilliams transform of the weight enumerator is defined in terms of the adjacency algebra of the scheme.

Next, in [3] Gabidulin proposed a slightly different definition of rank-metric code, in which the codewords are vectors over a finite extension of a finite field (where each coordinate can be replaced by the column vector of its coefficients over the base field obtaining hence a matrix and thus leading to a code in Delsarte's sense).

However, it was not until 2007 when MacWilliams identities were proved for Gabidulin-like rank-metric codes by Gadouleau and Yan in [4] and in full generality, namely, for Delsarte codes, by Ravagnani in [8]. Gadouleau and Yan's main contribution is a MacWilliams identity in the form of a closed MacWilliams transform for the original code where a strong use of the q-product and q-derivative is made, whilst Ravagnani's result exploits the perfect pairing character of the trace bilinear form and several combinatorial properties of the strict shortening operator to obtain a sequence of identities which relates the q-binomial moments of the primal and dual codes.

J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, V. Sotomayor (eds.): Proceedings of the XIX EACA, pp. 70-74 (2026). ISBN: 978-84-09-87277-0

This report is based on [1], where the reader can find all the details and additional results. The reader is also encouraged to consult [5] for a more detailed report of the contents presented here.

The goal of this report is to establish a relation between the coefficients of the weight enumerator polynomials of a code and its dual. This relation is intended as a first step toward deriving, in the future, a functional relationship between the corresponding polynomials.

Some preliminaries

To start with, for each ring R and integers $1 \leq n \leq m$, the set $M_{m,n}(R)$ of matrices with m rows and n columns can be regarded as an hermitian left $M_m(R)$-module with sesquilinear form b given by $b(X,Y) := \mathrm{Tr}(XY^t)$, where $M_m(R)$ is the set of matrices with m rows and one column and is regarded as ring with involution given by matrix transposition.

Definition 1 (The dual of a submodule)**.** Given a submodule $\mathcal{C} \subset M_{m,n}(R)$ (or more in general, just a subset), its dual is defined as

$$\mathcal{C}^{\perp} := \{Y \in M_{m,n}(R) : \ b(X,Y) = 0 \text{ for all } X \in \mathcal{C}\}.$$

Recall that a chain ring is a local ring with maximal ideal generated by a single nilpotent element.

Definition 2 (Code of rank k)**.** Let R be a chain ring. A code $\mathcal{C}$ in $M_{m,n}(R)$ is defined as a free R-submodule of $M_{m,n}(R)$. We will say $\mathcal{C}$ is a code with rank k if $\mathcal{C}$ is a free R–module of rank k.

Remark 3. Given a word A of a code, we will denote by $\mathrm{RS}(A)$ the submodule generated by the rows of A.

Definition 4 (Minimum distance)**.** Given $\mathcal{C}$ a code of rank k in $M_{m,n}(R)$ and $A \in \mathcal{C}$ a word, the rank of A, $\mathrm{rank}(A)$, is the cardinal of a minimal set of generators of $\mathrm{RS}(A)$. The minimum distance of $\mathcal{C}$ is defined as $d(\mathcal{C}) := \min\{\mathrm{rank}(U) \mid U \in \mathcal{C} \setminus \{O\}\}$, where O denotes the zero matrix.

Definition 5 (The weight enumerator)**.** Let $\mathcal{C}$ be a code of rank k in $M_{m,n}(R)$ of minimal distance d. For $d \leq t \leq n$, denote $W_t(C) = |\{X \in C : \ \mathrm{rank}(X) = t\}|$. The weight enumerator of $\mathcal{C}$ is defined as

$$W_{\mathcal{C}}(x,y) = x^n + \sum_{t=d}^{n} W_t(\mathcal{C}) x^{n-t} y^t.$$

Hereafter, $W_t(\mathcal{C})$ will be denoted as A_t, and $W_t(\mathcal{C}^{\perp})$ will be denoted by B_t.

Theorem 6 (Singleton bound)**.** *Let R be a local ring and let $\mathcal{C} \subseteq \mathcal{M}_{m,n}(R)$ be a code over R with minimum distance d. Then,*

$$|\mathcal{C}| \leq |R|^{\min\{n(m-(d-1)),\ m(n-(d-1))\}}.$$

A code that attains the Singleton bound is called a *maximum rank distance* code, abbreviated as **MRD**.

Definition 7 (q-binomial coefficient)**.**

$$\binom{n}{k}_q = \begin{cases} \frac{[n]_q!}{[k]_q![n-k]_q!} & \text{if } k \leq n, \\ 0, & \text{if } k > n. \end{cases}$$

Where $[n]_q = 1 + q + q^2 + \cdots + q^{n-1} = \begin{cases} \frac{(1-q^n)}{1-q} & \text{if } q \neq 1, \\ n & \text{if } q = 1. \end{cases}$

Main result and some consequences

To achieve our goal, we use counting techniques based on the fact that the weight enumerators of a code of rank k are determined by the number of codewords of weight $u \leq k$. This reduces the problem to counting matrices whose row support is contained in a free module of fixed dimension, which leads us to study free R-submodules of prescribed rank inside R^n.

Theorem 8. *Let R be a chain ring with maximal ideal $\mathfrak{m}$ and finite residue field with q elements. Then, the number of free R-linear submodules of rank k' of a given R-linear code of rank k is given by*

$$\begin{Bmatrix} k \\ k' \end{Bmatrix} = |\mathfrak{m}|^{k'(k-k')} \binom{k}{k'}_q.$$

Definition 9. Let R be a chain ring, $\mathcal{C} \subseteq M_{m,n}(R)$ a code, and $U \subseteq R^n$ a free R-submodule. The following sets are defined:

$$R_U := \{X \in M_{m,n}(R) \mid \mathsf{RS}(X) \subseteq U\}, \qquad \mathcal{C}_U := \{X \in \mathcal{C} \mid U \subseteq \ker(X)\}.$$

Lemma 10. *Let R be a chain ring and let $U \subseteq R^n$ be a free R-submodule of rank $n - u$. Then*

$$|\mathcal{C}_U| = \frac{|\mathcal{C}|\,|(\mathcal{C}^\perp)_{U^\perp}|}{|R|^{m(n-u)}}.$$

Lemma 11. *Let R be a local ring with maximal ideal $\mathfrak{m}$ and residue field with q elements. Consider integers $0 \leq t \leq s \leq k$. Let X be a free R-submodule of R^k with $\mathsf{rank}(X) = t$. Then, the number of free R-submodules $U \subseteq R^k$ such that $X \subseteq U$ and $\mathsf{rank}(U) = s$ is*

$$\begin{Bmatrix} k-t \\ k-s \end{Bmatrix}.$$

This lemma provides the key to our counting problem. It allows us to compute the weight enumerators of a code by counting the free submodules of R^n.

Lemma 12. *Suppose that R is a chain ring and that $\mathcal{C} \subseteq \mathcal{M}_{m,n}(R)$ is a code with weight distribution $(A_i)_{i=1}^n$. Let $0 \leq s \leq n$. Then*

$$\sum_{\substack{\mathsf{rank}(U)=s \\ U \text{ free in } R^n}} |\mathcal{C} \cap R_U| = \sum_{i=0}^{n} A_i \begin{Bmatrix} n-i \\ n-s \end{Bmatrix}.$$

The next result may be regarded as a generalization of [4, Proposition 4] and [8, Theorem 31]; it relates the binomial moments of the rank distributions of $\mathcal{C}$ and $\mathcal{C}^\perp$. This is the main result of this report.

Theorem 13 (Binomial moments for the rank distribution)**.** *Let R be a chain ring, and let $\mathcal{C} \in M_{m,n}(R)$ be a rank metric code. Moreover, let (A_i) and (B_i) be the weight distributions of $\mathcal{C}$ and $\mathcal{C}^\perp$ respectively. Then, for any $0 \leq \nu \leq n$, we have*

$$\sum_{i=0}^{n-\nu} A_i \begin{Bmatrix} n-i \\ \nu \end{Bmatrix} = \frac{|\mathcal{C}|}{|R|^{m\nu}} \sum_{j=0}^{\nu} B_j \begin{Bmatrix} n-j \\ \nu-j \end{Bmatrix}.$$

The proof is given by using Lemmas 10 and 11. One elementary consequence of Theorem 13 is the following statement, which recovers and extends [8, Corollary 33].

Corollary 14. *Let $\mathcal{C}$ be an $[m \times n, k, d]$ code over a chain ring R, and let $(A_i)_i$, $(B_j)_j$ be respectively the rank distributions of $\mathcal{C}$ and $\mathcal{C}^\perp$. Given $0 \leq \nu \leq n$, set*

$$a(\nu, n) := \frac{|R|^{m\nu}}{|\mathcal{C}|} \sum_{i=0}^{n-\nu} A_i \begin{Bmatrix} n-i \\ \nu \end{Bmatrix}.$$

Then, the B_j's are given by the recursive formula

$$B_0 = 1, \quad B_\nu = a(\nu, n) - \sum_{j=0}^{\nu-1} B_j \begin{Bmatrix} n-j \\ \nu-j \end{Bmatrix} \text{ if } 1 \leq \nu \leq n, \quad B_\nu = 0, \text{ if } \nu > n.$$

Finally, we establish, as announced, that the MRD character is preserved by duality:

Theorem 15. *If $\mathcal{C}$ is an MRD code, then so is $\mathcal{C}^\perp$.*

Acknowledgements. The first author received partial support by grant PID2022-136944NB-I00 funded by MICIU/AEI/10.13039/501100011033, and by grant PID2022-137283NB-C22 funded by MICIU/AEI/10.13039/501100011033.

References

[1] I. Blanco-Chacón, A.F. Boix, M. Greferath, E. Hieta-Aho: MacWilliams duality for rank metric codes over finite chain rings. *Finite Fields Appl.* **103**, 102584, 22 pp. (2025).

[2] P. Delsarte: Bilinear forms over a finite field, with applications to coding theory. *J. Combin. Theory Ser. A* **25**(3), 226–241 (1978).

[3] È.M. Gabidulin: Theory of codes with maximum rank distance. *Probl. Inf. Transm.* **21**, 1–12 (1985).

[4] M. Gadouleau, Z. Yan: MacWilliams identity for codes with the rank metric. *J. Wireless Com. Network* **2008**, 754021, 1–13 (2008).

[5] V. García Benítez: *Códigos con métrica de rango sobre anillos de Galois*. Master's thesis, Universidad de Granada (2025).

[6] J. MacWilliams: A theorem on the distribution of weights in a systematic code. *Bell System Tech. J.* **42**, 79–94 (1963).

[7] F.J. MacWilliams, N.J.A. Sloane, J.M. Goethals: The MacWilliams identities for nonlinear codes. *Bell System Tech. J.* **51**, 803–819 (1972).

[8] A. Ravagnani: Rank-metric codes and their duality theory. *Des. Codes Cryptogr.* **80**(1), 197–216 (2016).

A COMBINATORIAL APPROACH TO THE BIRATIONAL GEOMETRY OF POINT BLOW-UPS OF THE PROJECTIVE SPACE

M.C. Brambilla*, O. Dumitrescu†, E. Postinghel‡, L.J. Santana Sánchez◇ℓ

◇ *Speaker at EACA 2026*

* *Università Politecnica delle Marche*

† *University of North Carolina at Chapel Hill, and Institute of Mathematics of the Romanian Academy "Simion Stoilow" IMAR*

‡ *Dipartimento di Matematica, Università degli Studi di Trento*

ℓ *Departamento de Matemáticas, Estadística e I.O., IMAULL, Universidad de La Laguna*

m.c.brambilla@univpm.it, dolivia@unc.edu, elisa.postinghel@unitn.it, lsantans@ull.edu.es

Abstract. We study the birational geometry of X_s^n, the blow-up of $\mathbb{P}^n_{\mathbb{C}}$ at s points in general position. We do so by identifying a set of stable base locus subvarieties, which we call Weyl r-planes, that arise as elements of the orbit of a fixed linear cycle under the action of the Weyl group on r-cycles. To every Weyl r-plane we associate a pseudoeffective curve class and, for fixed r and $s \geq n+3$, all such classes form an orbit for a formal Weyl action on 1-cycles.

INTRODUCTION

Let X_s^n denote the complex projective space $\mathbb{P}^n$ blown up at s general points. The birational geometry of these varieties has attracted the attention of many authors over the last decades. First of all, we recall that a complete classification of those that are Mori dream spaces is known due to [4] and [3]:

$$X_s^2 \text{ for } s \leq 8;\ X_s^3 \text{ for } s \leq 7;\ X_s^4 \text{ for } s \leq 8;\ X_s^n \text{ for } n \geq 5 \text{ and } s \leq n+3.$$

The nice feature of Mori dream spaces is that the effective cone of divisors is rational polyhedral and it admits a subdivision into finitely many nef chambers which fully describes its birational geometry. In the case of Mori dream spaces of type X_s^n, the Mori chamber decomposition is given by a hyperplane arrangement where each hyperplane corresponds dually to a curve class. In this work we prove that these curve classes fit in some orbit, for a formal Weyl action on 1-cycles, of curves of type

$$c_I = (|I|-1)h - \sum_{i \in I} e_i, \tag{1}$$

where $I \subset \{1, \dots, s\}$ is an index subset of length $|I| \leq n$. This provides a combinatorial tool which can be extended to non-Mori dream spaces X_s^n to study the birational geometry of these spaces.

J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, V. Sotomayor (eds.): Proceedings of the XIX EACA, pp. 75-77 (2026). ISBN: 978-84-09-87277-0

The Weyl action

The Néron-Severi space $\mathsf{N}^1(X_s^n)_{\mathbb{R}}$ is spanned by the general hyperplane class H and by the exceptional divisors E_i, thus any divisor class in X_s^n can be written as a linear combination

$$D = dH - \sum_{i=1}^{s} m_i E_i. \tag{2}$$

The *standard Cremona transformation based on the coordinate points* of $\mathbb{P}^n$ is the birational transformation defined by the rational map:

$$\mathsf{Cr} := (x_0 : \cdots : x_n) \mapsto (x_0^{-1} : \cdots : x_n^{-1}).$$

Assuming that $s \geq n+1$, given any subset $\Gamma \subseteq \{1, \ldots, s\}$ of cardinality $n+1$, we denote by Cr_Γ and call *standard Cremona transformation* the map obtained by precomposing Cr with a projective transformation which takes the points indexed by Γ to the coordinate points of $\mathbb{P}^n$. A standard Cremona transformation induces an automorphism of $\mathsf{N}^1(X_s^n)_{\mathbb{R}}$, denoted again by Cr_Γ by abuse of notation, by sending a divisor (2) to

$$\mathsf{Cr}_{\Gamma(D)} = (d - b_\Gamma)H - \sum_{i \in \Gamma}(m_i - b_\Gamma)E_i - \sum_{i \notin \Gamma} m_i E_i,$$

where

$$b_{\Gamma(D)} = b_\Gamma := \sum_{i \in \Gamma} m_i - (n-1)d.$$

The *Weyl group* W_s^n is the group generated by the standard Cremona transformations.

Let $\mathsf{N}_1(X_s^n)_{\mathbb{R}} = (A_1(X_s^n)/\equiv) \otimes \mathbb{R}$ be the space of numerical equivalence classes of 1-cycles, which is dual to the Néron-Severi space $\mathsf{N}^1(X_s^n)_{\mathbb{R}}$ with respect to the standard intersection pairing. A basis of $\mathsf{N}_1(X_s^n)_{\mathbb{R}}$ is given by $h = H^{n-1}$, the general line class in X_s^n, and, for $i = 1 \ldots, s$, by e_i, the class of a general line inside the exceptional divisor E_i. Thus, the intersection product of a divisor $D \in \mathsf{N}^1(X_s^n)_{\mathbb{R}}$ of the form (2) and a 1-cycle c in $\mathsf{N}_1(X_s^n)_{\mathbb{R}}$ of class

$$c = \delta h - \sum_{i=1}^{s} \mu_i e_i, \tag{3}$$

is computed by

$$D \cdot c = d\delta - \sum_{i=1}^{s} m_i \mu_i.$$

The Weyl action on the Néron-Severi space formally induces an action on 1-cycle classes by duality as follows. Fix an index set $\Gamma \subset \{1, \ldots, s\}$ of length $n+1$. For a given $c \in \mathsf{N}_1(X_s^n)_{\mathbb{R}}$, the class $\mathsf{Cr}_{\Gamma(c)} \in \mathsf{N}_1(X_s^n)_{\mathbb{R}}$ is defined by the condition

$$\mathsf{Cr}_{\Gamma(D)} \cdot \mathsf{Cr}_{\Gamma(c)} = D \cdot c,$$

for every $D \in \mathsf{N}^1(X_s^n)_{\mathbb{R}}$. Explicitly, the group element $\mathsf{Cr}_\Gamma \in W_s^n$ takes the 1-cycle class (3) to

$$\mathsf{Cr}_{\Gamma(c)} = (\delta - (n-1)a_\Gamma)h - \sum_{i \in \Gamma}(\mu_i - a_\Gamma)e_i - \sum_{i \notin \Gamma} \mu_i e_i.$$

where

$$a_{\Gamma(c)} = a_\Gamma := \sum_{i \in \Gamma} \mu_i - \delta.$$

The Weyl chamber decomposition

The main result of this talk highlights how the Weyl action on 1-cycle classes completely governs the birational geometry of X_s^n when it is a Mori dream space. Thanks to the nature of the Weyl action, this yields a combinatorial approach to this problem. Namely, let us consider the set of 1-cycle classes:

$$\{w(c_I) : w \in W_s^n,\ I \subset \{1, \dots, s\},\ 2 \leq |I| \leq n\},$$

where c_I is as defined in 1 and W_s^n is the Weyl group. We consider the hyperplane arrangement in the Néron-Severi space given by

$$\{D \cdot w(c_I) = 0 : w \in W_s^n, I \subset \{1, \dots, s\}, 2 \leq |I| \leq n\}. \tag{4}$$

Definition 1. The *Weyl chamber decomposition* is the wall-and-chamber decomposition of the pseudoeffective cone of divisors of X_s^n induced by the hyperplane arrangement (4).

The Mori chamber decomposition of X_s^n in the Mori dream space case was studied by Mukai and is explicitely described in [1, Theorem 5.1] when $s = n + 3$.

Theorem 2. *Let X_s^n be a Mori dream space, then the Mori and the Weyl chamber decompositions agree.*

When X_s^n is not a Mori dream space, the Weyl chamber decomposition is given by infinitely many walls and we conjecture that it nevertheless provides a nef chamber decomposition in the negative part of the pseudoeffective cone when $s = n + 4$. We ask whether the same holds true for a general X_s^n.

All the results of this talk can be found in [2].

Acknowledgements. The first author has been partially supported by the European Union Next Generation EU, M4C1, CUP E53C24002320006 - 2022NBN7TL - Applied Algebraic Geometry of Tensors. The second author has been partially supported by the NSF-FRG DMS 2152130 grant. The third author has been partially supported by the European Union Next Generation EU, Mission 4, Component 2 - CUP E53D23005400001.

References

[1] M.C. Brambilla, O. Dumitrescu, E. Postinghel, L. Santana Sanchez: Duality and polyhedrality of cones for Mori dream spaces. *Math. Z.* **309**, 69 (2025).

[2] M.C. Brambilla, O. Dumitrescu, E. Postinghel, L. Santana Sanchez: Birational geometry of blowups via Weyl chamber decompositions and actions on curves. *ArXiv:2410.18008v3* (2025).

[3] A.M. Castravet, J. Tevelev: Hilbert's 14th problem and Cox rings. *Compos. Math.* **142**(6), 1479–1498 (2006).

[4] S. Mukai: Counterexample to Hilbert's fourteenth problem for the 3-dimensional additive group. *RIMS Preprint* (2001).

Quadratic exchange equations for Coxeter matroids

K. Calvert*, A. Dermenjian◇†, A. Fink‡, B. Smith*

◇ *Speaker at EACA 2026*

* *Lancaster University*

† *Universidad de Sevilla*

‡ *Queen Mary University of London*

kieran.calvert@lancaster.ac.uk, aram.dermenjian.math@gmail.com, a.fink@qmul.ac.uk, b.smith9@lancaster.ac.uk

Abstract. Tropicalisation (with trivial coefficients) is a process that turns a polynomial equation into a combinatorial predicate on subsets of the set of variables. We show that for each minuscule representation of a simple reductive group, there is a set of quadratic equations cutting out the orbit of the highest weight vector whose tropicalisation characterises the set of Coxeter matroids for that representation which satisfy the strong exchange property. In this extended abstract we focus on type B, with all other types being handled in our forthcoming paper.

Introduction

A linear space of dimension r over $\mathbb{C}^n$ represents a matroid of rank r on the ground set $\{1,\dots,n\}$ and these linear spaces are parametrised by $\mathbb{C}$-valued points of the Grassmannian $\mathrm{Gr}(r,n)$. This relationship between the Grassmannian and matroids is used to great profit in the overlap of algebraic geometry and combinatorics, for example in tropical geometry. The *quadratic (Grassmann–)Plücker relations* are a certain set of quadrics coming from the Grassmannian whose tropicalisation gives us a realisation of the matroid polytope.

Many have studied how well this happy state of affairs replicates for other quotients $\mathbb{G}/\mathbb{P}$ of a reductive group by a parabolic subgroup. A similar approach works for $\mathbb{G}/\mathbb{P}$ using a projectivised $\mathbb{G}$-representation $\mathrm{proj}(V_\lambda)$ to give quadrics. We say V_λ is *minuscule* if all the weights of V_λ are in a single Coxeter group orbit. In this extended abstract, we focus exclusively on when V_λ is minuscule.

On the other side of the connection, *Coxeter matroids* [1] are to $\mathbb{G}/\mathbb{P}$ as matroids are to the Grassmannian. A Coxeter matroid is any subpolytope of the orbit polytope for $\mathbb{P}$ of the Coxeter group $W(\mathbb{G})$ whose edges are parallel to roots of $\mathbb{G}$. In our paper we show:

Theorem 1. *For $\mathbb{G}$ a simply connected complex Lie group and $\mathbb{P}$ a minuscule parabolic subgroup. There is a set Q spanning the quadrics cutting out $\mathbb{G}/\mathbb{P} \subset \mathrm{proj}(V_\lambda)$ such that*

J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, V. Sotomayor (eds.): Proceedings of the XIX EACA, pp. 78-82 (2026).
ISBN: 978-84-09-87277-0

a set is the vertex set of a strong Coxeter matroid if and only if it satisfies the equations $\mathrm{trop}(Q)$.

The one word yet to be defined is «strong». We say that a Coxeter matroid P is *strong* if for any two vertices v, w of P, either $\mathrm{conv}\{v, w\}$ is parallel to a root or it is the diagonal of a parallelogram all four of whose vertices are vertices of P. (Such Coxeter matroids are also said to satisfy the *strong exchange property*). In this abstract we focus only on the computational/combinatorial side of type B Coxeter matroids and exclude the representation theory part to fit the audience. The calculations for the quadrics, the representation theory, the other types and all proofs can be found in [2].

Coxeter matroids

In this section we fix notation for Coxeter matroids. For a more thorough introduction, the interested reader is invited to look at [1, 4].

Coxeter groups

Let $\mathcal{V}$ be an n-dimensional Euclidean real vector space with inner product $(\cdot, \cdot)$. For a given hyperplane $H \subset \mathcal{V}$, we let s_H denote the reflection which fixes H pointwise and sends a normal vector of H to its opposite. A *Coxeter group* W is a finite group generated by a set of reflections in the orthogonal group $O(\mathcal{V})$. A *reflecting hyperplane* for W is a hyperplane H such that $s_H \in W$. The set of reflecting hyperplanes of W forms the *Coxeter arrangement of* W.

For a given W we consider a *root system* $\Phi \subset \mathcal{V}$ and let Φ^+ and Φ^- denote the set of *positive roots* and *negative roots* respectively. We let $\Pi \subseteq \Phi^+$ denote the set of *simple roots* and $S \subseteq W$ consist of the reflections with a simple root as a normal vector, named the *simple reflections*. Then S generates W. We will require our root systems be crystallographic: they satisfy $\frac{2(\alpha,\beta)}{(\beta,\beta)} \in \mathbb{Z}$ for all $\alpha, \beta \in \Phi$.

For a given subset $J \subseteq S = \{s_1, \ldots, s_n\}$, we let $P_J = \langle J \rangle$ be the *standard parabolic subgroup of* W *generated by* J and $W^J = W/P_J$ denote the *standard parabolic cosets*. The *maximal parabolic subgroups* are precisely the standard parabolic subgroups of W where $J = S \setminus \{s_i\}$ for some $i \in [n]$. In this abstract we focus on maximal parabolic subgroups $P_J = S \setminus \{s_i\}$ which are minuscule. To avoid the representation theory, we do not give a precise definition of minuscule and instead refer the reader to [3] or [2].

Coxeter matroids

For a given standard parabolic subgroup P_J, we choose a point $\omega_J \in V$ such that ω_J is in the intersection of all hyperplanes of the Coxeter arrangement restricted to the parabolic subgroup and is in the negative half-space of the rest. The choice of ω_J allows us to define an injective map from cosets W^J to the vector space $\mathcal{V}$ under which $wP_J \mapsto w \cdot \omega_J$. Thus, we will write $A \cdot \omega_J$ for the point associated to the coset $A \in W^J$.

Given a subset $M \subseteq W^J$, we let $P(M)$ be the polytope constructed by taking the convex hull of $A \cdot \omega_J$ for all $A \in M \subseteq W^J$. When $M = W^J$, we call $P(M) = \text{conv}\{W \cdot \omega_J\}$ the *ambient polytope of* W^J. We say that M is a *Coxeter matroid* if and only if every edge of $P(M)$ is parallel to a root in Φ.

The *strong exchange property for Coxeter matroids* is the following property that a Coxeter matroid $M \subseteq W^J$ may have: for any distinct cosets A, B in $M \subseteq W^J$ there is a reflecting hyperplane H separating A and B such that $s_H A, s_H B \in M$. We say a Coxeter matroid is *strong* if it satisfies the strong exchange property. In fact the strong exchange property is a sufficient condition for an arbitrary subset $M \subseteq W^J$ to form a Coxeter matroid.

Type B Coxeter matroids

The root system of B_n has the following choices of simple roots $\Pi(B_n) = \{\alpha_i := e_i - e_{i+1} \mid 1 \leq i \leq n-1\} \cup \{\alpha_n := e_n\}$. For $W = W(B_n)$, the only minuscule parabolic subgroup is P_J where $J = S \setminus \{s_n\}$. By concretely choosing $\omega_J = (-\frac{1}{2}, \ldots, -\frac{1}{2})$, we see that the ambient polytope is the cube $[-\frac{1}{2}, \frac{1}{2}]^n$. For a set $I \subseteq [n]$, define $\varepsilon_I \in \mathcal{V} = \mathbb{R}^n$ to be the indicator vector of I translated by $(-\frac{1}{2}, \ldots, -\frac{1}{2})$. Then

$$Q_n := \{\varepsilon_I \mid I \subseteq [n]\} = W(B_n) \cdot \omega_{S \setminus \{s_n\}}, \quad (\varepsilon_I)_i = \begin{cases} -\frac{1}{2} & i \notin I \\ \frac{1}{2} & i \in I. \end{cases}$$

The ambient polytope is the cube obtained as the convex hull of these points.

Characterising strong Coxeter matroids

In this section we give a combinatorial characterisation of strong Coxeter matroids M in terms of tropical equations for type B. Recall we handle the other types (and the representation theory) in [2].

Tropical equations

We define tropical equations here in a bare-bones way. For context and a detailed treatment of tropical algebra, see [5].

Let $\mathbb{B} = (\{0, 1\}, \oplus, \odot)$ be the Boolean semifield, where 0 is the zero, 1 the multiplicative identity, and $1 \oplus 1 = 1$. Let X be a finite set of indeterminates. Then $\mathbb{B}[X]$ is the monoid semiring with coefficients in $\mathbb{B}$ of the free commutative monoid $\mathbb{N}^X = \text{Hom}_{\text{Set}}(X, \mathbb{N})$ on the generators X. Explicitly, for $a \in \mathbb{N}^X$, let $X^{\odot a}$ denote the formal monomial $\bigodot_{x \in X} \underbrace{x \odot \cdots \odot x}_{a(x) \text{ times}}$. Then every element of $\mathbb{B}[X]$ is of the form

$$\bigoplus_{a \in A} X^{\odot a}$$

for some finite subset $A \subset \mathbb{N}^X$. Addition in $\mathbb{B}[X]$ corresponds to union of the sets A, and multiplication to Minkowski sum. The *tropicalisation* map $\text{trop} : \mathbb{C}[X] \to \mathbb{B}[X]$ is defined by $\text{trop}(\sum_{a \in A} z_a X^a) = \bigoplus_{a \in A} X^{\odot a}$ where $z_a \in \mathbb{C}$ is nonzero for all $a \in A$.

When we call an element $f \in \mathbb{B}[X]$ a *tropical equation*, we are thinking of it as a condition that may or may not be satisfied by a tuple $p \in \mathbb{B}^X$. The tropical equation $f = \bigoplus_{a \in A} X^{\odot a}$ is *satisfied* by p if the number of $a \in A$ such that $p^{\odot a} = 1$ – i.e. such that $p(x) = 1$ for all x with $a(x) > 0$ – is not exactly 1.

The tropical equations arising in this section will have $X = \{x_S \mid S \subseteq [n]\}$. Set systems M on $[n]$ are in bijection with tuples $\nu_M \in \mathbb{B}^X$ by the rule that $\nu_M(x_S) = 1$ if and only if $S \in M$. In this way we may make sense of saying that a set system M satisfies a tropical equation $f \in \mathbb{B}[X]$: we mean that ν_M satisfies f.

Equations

The *type B strong exchange equations* on $[n]$ are the equations in the collection $\mathcal{F}_n^{(B)} := \{f_{I,J}^{(B)} \mid I, J \subseteq [n], |I \triangle J| \geq 3\}$ where

$$\begin{aligned} f_{I,J}^{(B)} &:= \textstyle\bigoplus_{i \in I \triangle J} x_{I \triangle i} \odot x_{J \triangle i} && \text{if } |I \triangle J| \equiv 0 \mod 2 \text{ and} \\ f_{I,J}^{(B)} &:= x_I \odot x_J \oplus \textstyle\bigoplus_{i \in I \triangle J} x_{I \triangle i} \odot x_{J \triangle i} && \text{if } |I \triangle J| \equiv 1 \mod 2. \end{aligned}$$

It turns out that the type B strong exchange equations precisely characterise strong Coxeter matroids of type B.

Theorem 2. *Let M be a set system on $[n]$. Then M is a strong Coxeter matroid of type B if and only if ν_M satisfies the type B strong exchange equations $\mathcal{F}_n^{(B)}$.*

This gives us a novel combinatorial way to view the strong exchange property of a type B Coxeter matroid. As mentioned, in [2] we also give a representation theory manner of finding these equations. Any missing definitions, notations, can be found in [2].

Theorem 3. *Let $\mathbb{G} = \mathrm{Spin}(2n+1)$ and $\mathbb{P}$ be a the maximal parabolic corresponding to the last fundamental weight. The type B quadratic embedding equations $\mathcal{E}_n^{(B)}$ are a spanning set for the equations of the embedding $\mathbb{G}/\mathbb{P} \subset \mathrm{proj}(\mathcal{S})$ and tropicalise to the type B strong exchange equations $\mathcal{F}_n^{(B)}$.*

Peerless antipodes

Let M be a type B Coxeter matroid and let $I, J \in M$ with matroid polytope $P(M)$. We define $\square_{I,J}$ to be the (smallest rank) hypercube which contains I and J We say $(\varepsilon_I, \varepsilon_J) \subseteq P(M)$ is a *peerless antipode* if it is the only antipode of $\square_{I,J}$ contained in $P(M)$. We say $(\varepsilon_I, \varepsilon_J) \subseteq P(M)$ is an *isolated antipode* if the restriction of $P(M)$ to $\square_{I,J}$ is exactly $(\varepsilon_I, \varepsilon_J)$. Note that, isolated antipodes are necessarily peerless, but the converse is not always true. We can characterise (2) in the following way.

Theorem 4. *Let M be a set system. Then M is a strong Coxeter matroid of type B if and only if it has no peerless antipode in any k-cube for $k \geq 3$.*

Furthermore, we can reduce this to the following

Proposition 5. *Let M be a Coxeter matroid of type B. Then M is a strong Coxeter matroid if and only if*

- *it has no peerless antipode in any 3-cube or 4-cube, and*
- *it has no isolated antipode in any k-cube for $k \geq 5$.*

Acknowledgements. The second author is part of the research project PID2022-138719NA-I00, financed by MCIN/AEI/10.13039/501100011033/FEDER, UE.

References

[1] A.V. Borovik, I.M. Gelfand, N. White: *Coxeter matroids*. Birkhäuser Boston (2003).

[2] K. Calvert, A. Dermenjian, A. Fink, B. Smith: Quadratic exchange equations for Coxeter matroids. *ArXiv:2511.13498* (2025).

[3] W. Fulton, J. Harris: *Representation theory*. Graduate Texts in Mathematics **129**, Springer New York (2004).

[4] J.E. Humphreys: *Introduction to Lie algebras and representation theory*. Graduate Texts in Mathematics, Springer New York (1972).

[5] D. Maclagan, B. Sturmfels: *Introduction to tropical geometry*. Graduate Studies in Mathematics **161**, American Mathematical Society (2015).

Equilibrium set of a two-protein toggle switch

E. Camacho-Aguilar*†, F. García-Cortés†, F.J. Castro-Jiménez◇†

◇ *Speaker at EACA 2026*

† *Universidad de Sevilla*

* *Centro Andaluz de Biología del Desarrollo*

ecamagu@us.es, fgarcia2@us.es, castro@us.es

Abstract. We employ symbolic and algebraic methods to analyze the equilibrium set of a two-protein toggle switch. We focus on how the geometry of this algebraic set changes as the parameters vary, aiming to provide a rigorous characterization of the bifurcation boundaries that govern biological decision-making.

Introduction

Understanding how complex gene networks produce specific morphologies remains a central challenge in developmental biology. These interactions are typically modeled via systems of ordinary differential equations (ODEs) using Hill functions to capture the sigmoidal nature of gene regulation. A fundamental goal is to characterize the *steady states* of these systems and their dependence on biological parameters, such as *interaction strengths* (**k**), *Hill coefficients* (**n**), and *production rates* (**v**). Even for small motifs such as the genetic toggle switch (a mutual repression system between two proteins x and y, see e.g. [4] and [3]), determining the number and stability of equilibria across the parameter space is computationally intensive. In this work, we employ symbolic and algebraic methods to analyze the equilibrium set of a two-protein toggle switch. We focus on how the geometry of this algebraic set changes as the parameters $(\mathbf{k}, \mathbf{n}, \mathbf{v})$ vary, aiming to provide a rigorous characterization of the bifurcation boundaries that govern biological decision-making.

We thank the referee for her/his useful comments.

Original question

In [2], following [1, App. p. 299], we studied a model for how a single morphogen could control cell differentiation into three cell types, where the gene expression in time is controlled by a certain dynamical system ([2, System (1)]). We were interested in understanding the set of equilibrium points $\mathcal{E}$ of previous dynamical system, depending on the parameters of the system. The algebraic set $\mathcal{E}$ is defined by a polynomial system given in ([2, System (2)]).

J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, V. Sotomayor (eds.): Proceedings of the XIX EACA, pp. 83-87 (2026).
ISBN: 978-84-09-87277-0

We study here a 2-dimensional analog of the previous situation, which has biological interest in itself, as mentioned in the introduction. Namely, assume k_{ij}, v'_i, $\{i,j\} = \{1,2\}$, are some non-zero complex numbers and consider the algebraic set defined in the affine complex plane by the system of equations

$$\begin{cases} f'_1 := x' \cdot \big(1 + (k_{21} \cdot y')^{n_{21}}\big) + v'_1 = 0, \\ f'_2 := y' \cdot \big(1 + (k_{12} \cdot x')^{n_{12}}\big) + v'_2 = 0, \end{cases}$$

where $n_{ij} \in \mathbb{Z}_{>0}$. To simplify notation, we write $\mathbf{k} = (k_{12}, k_{21})$, $\mathbf{v'} = (v'_1, v'_2)$ and $\mathbf{n} = (n_{12}, n_{21})$. We fix arbitrary $n_{ij} \in \mathbb{Z}_{>0}$. Considering $\mathbf{k}$ and $\mathbf{v'}$ as indeterminate, we may also look at the ideal $I' \subset \mathbb{C}[\mathbf{k}, \mathbf{v'}, x', y']$ generated by $\{f'_1, f'_2\}$. We denote $\mathcal{Z}' = \mathcal{V}(I')$ the corresponding algebraic set in the affine complex space $\mathbb{A}^6 = \mathbb{A}^6_{\mathbf{v},\mathbf{k},x',y'}$.

Reducing the number of variables

Assume we specialize the indeterminate k_{ij} to a non-zero complex number k^0_{ij}. To simplify notation, we write again k_{ij} instead of k^0_{ij}. First observe that, after multiplying the i-th equation by k_{ij}, redefining $v_i := k_{ij}\, v'_i$ and applying the change of variables $x := k_{12}\, x'$, $y := k_{21}\, y'$, we obtain the algebraic set

$$\mathcal{Z} := \mathcal{V}\big(f_1, f_2\big) \subset \mathbb{A}^4_{\mathbf{v},x,y},$$

where

$$f_1 = x(1 + y^{n_{21}}) + v_1, \quad f_2 = y(1 + x^{n_{12}}) + v_2,$$

both polynomials in $\mathbb{C}[\mathbf{v}, x, y]$. It is obvious that we can recover $\mathcal{Z}' \cap \{k_{ij} \neq 0\}$ from $\mathcal{Z}$. We restrict ourself to the study of $\mathcal{Z}$. The cases where at least one of the n_{ij} is 1 are special (but still meaningful in Biology).

We consider the projection $\pi_1 : \mathbb{A}^4_{\mathbf{v},x,y} \to \mathbb{A}^2_{\mathbf{v}}$. As we shall prove in Proposition 3 that the restriction $\rho_1 := \pi_1|_{\mathcal{Z}}$ is dominant. We are interested in a complete understanding of the fibers of the morphism

$$\rho_1 : \mathcal{Z} \to \mathbb{A}^2_{\mathbf{v}}.$$

In the following, we use explicit methods from commutative algebra.

General study of $\mathcal{Z} \subset \mathbb{A}^4_{\mathbf{v},x,y}$

Define further the ideal $I_f (= I) := (f_1, f_2) \subset \mathbb{C}[\mathbf{v}, x, y]$, which is a prime ideal since the quotient ring $\mathbb{C}[\mathbf{v}, x, y]/I$ is isomorphic to $\mathbb{C}[x, y]$. So, the algebraic set $\mathcal{Z} \subset \mathbb{A}^4_{\mathbf{v},x,y}$ is a 2-dim'l irreducible algebraic variety.

Another presentation of I_f after localization

Consider the polynomials

$$g_1 := (1 + x^{n_{12}})^{n_{21}}(x + v_1) + (-v_2)^{n_{21}} x,$$
$$g_2 := -(-v_2)^{n_{21}-1}(y + v_2) + x^{n_{12}-1}(1 + x^{n_{12}})^{n_{21}-1}(x + v_1)$$

in $\mathbb{C}[\mathbf{v}, x, y]$. Let $I_g := (g_1, g_2) \subset \mathbb{C}[\mathbf{v}, x, y]$.

A direct computation proves the inclusion $I_g \subset I_f$. Indeed, let us consider the matrix

$$M = \begin{pmatrix} (1+x^{n_{12}})^{n_{21}} & -x\frac{(f_2-v_2)^{n_{21}}-(-v_2)^{n_{21}}}{f_2} \\ x^{n_{12}-1}(1+x^{n_{12}})^{n_{21}-1} & y\frac{(f_2-v_2)^{n_{21}-1}-(-v_2)^{n_{21}-1}}{f_2} - \frac{(f_2-v_2)^{n_{21}}-(-v_2)^{n_{21}}}{f_2} \end{pmatrix}.$$

Notice that M has entries in $\mathbb{C}[\mathbf{v}, x, y]$ and that

$$M \cdot \begin{pmatrix} f_1 \\ f_2 \end{pmatrix} = \begin{pmatrix} g_1 \\ g_2 \end{pmatrix}.$$

We have

$$|M| = -(-v_2)^{n_{21}-1}(1+x^{n_{12}})^{n_{21}-1},$$

and then

$$|M| \cdot \begin{pmatrix} f_1 \\ f_2 \end{pmatrix} = \mathsf{adj}(M) \cdot \begin{pmatrix} g_1 \\ g_2 \end{pmatrix}.$$

This is enough to prove that

$$S^{-1}(g_1, g_2) = S^{-1}(f_1, f_2) \subset S^{-1}\mathbb{C}[\mathbf{v}, x, y],$$

if $S \subset \mathbb{C}[\mathbf{v}, x, y]$ be the multiplicative set generated by v_2. Notice that the choice of g_1, g_2 broke the symmetry of the ideal I_f.

Elimination ideals

Elimination of the variables v_1, v_2: Take any monomial ordering on $\mathbb{C}[v_1, v_2, x, y]$ such that $v_1 > v_2 >$ (any other variable). Then it is clear that $\{f_1, f_2\}$ is a Gröbner basis of I_f and we can inmediately compute:

$$I_f \cap \mathbb{C}[v_2, x, y] = (f_2) \text{ and } I_f \cap \mathbb{C}[x, y] = (0).$$

Similarly for $v_2 > v_1$:

$$I_f \cap \mathbb{C}[v_1, x, y] = (f_1).$$

Elimination of the variables x, y:

Proposition 1. $I_f \cap \mathbb{C}[\mathbf{v}, x] = (g_1)$.

Proof. The generic computation: Set $K := \mathbb{C}(\mathbf{v})$ and $J := I_f K[x, y]$. Since $v_2 \in K^\times$, it follows that the set $\{g_2, g_1\}$ is a Gröbner basis of the ideal J with respect to the lexicographical order with $y < x$. By *Elimination theory* we find $J \cap K[x] = (g_1)$.
Removal of the generic hypothesis: Lef $h \in I_f \cap \mathbb{C}[\mathbf{v}, x]$ and write $h = p \cdot f_1 + q \cdot f_2$. After multiplication by a polynomial $c_h(v_2) \in \mathbb{C}[v_2]$ (in fact, the monomial $v_2^{2(n_{21}-1)}$ works) we obtain $c_h(v_2) \cdot h \in (g_1, g_2)$.

We look at the equality $c_h(v_2)h = c_h(v_2)p \cdot f_1 + c_h(v_2)q \cdot f_2$ in the ring $K[x, y]$. After the previous item, g_1 divides $c_h(v_2)h$ in $K[x]$, say $c_h(v_2)h = u \cdot g_1$ for some $u \in K[x]$, and take $c_u \in \mathbb{C}[\mathbf{v}]$ such that $c_u \cdot u \in \mathbb{C}[\mathbf{v}, x]$.

Then $c_u c_h \cdot h = c_u u \cdot g_1$. Since $c_u c_h \in \mathbb{C}[\mathbf{v}]$ but $\deg_x g_1 = n_{12}n_{21} + 1 > 1$, it follows that g_1 divides h in $\mathbb{C}[\mathbf{v}, x]$. Therefore $I_f \cap \mathbb{C}[\mathbf{v}, x] = (g_1)$. □

Corollary 2. $I_f \cap \mathbb{C}[\mathbf{v}] = (0)$.

Corollary 3. *The morphism* $\rho_1 : \mathcal{Z} \to \mathbb{A}^2_{\mathbf{v}}$ *is dominant, i.e.* $\overline{\rho_1(\mathcal{Z})}^{\text{Zar}} = \mathbb{A}^2_{\mathbf{v}}$.

Proof. This is equivalent to the ring homomorphism

$$\mathbb{C}[\mathbf{v}] \hookrightarrow \mathbb{C}[\mathbf{v}, x, y] \twoheadrightarrow \frac{\mathbb{C}[\mathbf{v}, x, y]}{I_f}$$

being injective, i.e. $I_f \cap \mathbb{C}[\mathbf{v}] = (0)$. □

A GEOMETRIC PICTURE

Symmetrizing previous construction, let us consider

$$g_1^{(1)} := (1 + y^{n_{21}})^{n_{12}}(y + v_2) + (-v_1)^{n_{12}} y,$$
$$g_2^{(1)} := (-v_1)^{n_{12}-1}(x + v_1) + y^{n_{21}-1}(1 + y^{n_{21}})^{n_{12}-1}(y + v_2);$$

and

$$g_1^{(2)} := (1 + x^{n_{12}})^{n_{21}}(x + v_1) + (-v_2)^{n_{21}} x,$$
$$g_2^{(2)} := (-v_2)^{n_{21}-1}(y + v_2) + x^{n_{12}-1}(1 + x^{n_{12}})^{n_{21}-1}(x + v_1).$$

Let $I_g^{(i)} := (g_1^{(i)}, g_2^{(i)}) \subset \mathbb{C}[\mathbf{v}, x, y]$ and $\mathcal{V}_g^{(i)} := \mathcal{V}(I_g^{(i)}) \subset \mathbb{A}^4_{\mathbf{v},x,y}$ for $i = 1, 2$. Write $\mathcal{V}_f := \mathcal{Z} = \mathcal{V}(I_f) \subset \mathbb{A}^4_{\mathbf{v},x,y}$.

Finally, let $\mathcal{V}^{(1)}_{g,\neg x} := \mathcal{V}(g_1^{(1)}) \subset \mathbb{A}^3_{\mathbf{v},y}$ (resp. $\mathcal{V}^{(2)}_{g,\neg y} := \mathcal{V}(g_1^{(2)}) \subset \mathbb{A}^3_{\mathbf{v},x}$) where $g_1^{(1)}$ (resp. $g_1^{(2)}$) is considered as an element of $\mathbb{C}[\mathbf{v}, y]$ (resp. $\mathbb{C}[\mathbf{v}, x]$). The results proven before are summarized in the diagram.

$$\begin{array}{ccccccc}
 & & \mathcal{V}^{(1)}_{g,\neg x} & \subset & \mathbb{A}^3_{\mathbf{v},y} & \xrightarrow{\pi_1} & \mathbb{A}^2_{\mathbf{v}} \\
 & & \uparrow{\scriptstyle \pi_{\neg x}} & & \uparrow{\scriptstyle \pi_{\neg x}} & & \uparrow{\scriptstyle \pi_1} \\
\mathcal{V}_g^{(1)} \cap \mathsf{D}(v_1) & \subset & \mathcal{V}_g^{(1)} & \subset & \mathbb{A}^4_{\mathbf{v},x,y} & \xrightarrow{\pi_{\neg y}} & \mathbb{A}^3_{\mathbf{v},x} \\
\| & & \cup & & \cup & & \cup \\
\mathcal{V}_f \cap \mathsf{D}(v_1) & \subset & \mathcal{V}_f & \subset & \mathcal{V}_g^{(2)} & \xrightarrow{\pi_{\neg y}} & \mathcal{V}^{(2)}_{g,\neg y} \\
 & & \cup & & \cup & & \\
 & & \mathcal{V}_f \cap \mathsf{D}(v_2) & = & \mathcal{V}_g^{(2)} \cap \mathsf{D}(v_2) & &
\end{array}$$

Acknowledgements. The first author has been partially supported by RYC2023-043012-I and CEX2020-001088-M. The second and third authors have been partially supported by Proyecto PID2020-117843GB-I00, and Proyecto PID2024-156912N funded by MICIU/AEI/10.13039/501100011033, and FEDER, UE.

REFERENCES

[1] E. Camacho-Aguilar, A. Warmflash: Insights into mammalian morphogen dynamics from embryonic stem cell systems. *Current topics in developmental biology* **137**, 279–305 (2020).

[2] E. Camacho-Aguilar, F.J. Castro-Jiménez, F. García-Cortés: *Algebraic methods in cell differentiation*. Book of Abstracts, EACA 2024, San Lorenzo del Escorial, 34–37 (2024).

[3] J.L. Cherry, F.R. Adler: How to make a Biological Switch. *J. Theor. Biol.* **203**(2), 117–133 (2000).

[4] T. Gardner, C. Cantor, J. Collins: Construction of a genetic toggle switch in Escherichia coli. *Nature* **403**, 339–342 (2000).

The Clifford defect of a numerical semigroup

E. Camps-Moreno*†, A. Fidalgo-Díaz◇‡, U. Martínez-Peñas‡, G.L. Matthews†

◇ *Speaker at EACA 2026*

* *Institut Mathématiques de Bordeaux*

† *Virginia Polytechnic Institute*

‡ *University of Valladolid*

eduardo.camps-moreno@math.u-bordeaux.fr, adrian.fidalgo22@uva.es, umberto.martinez@uva.es, gmatthews@vt.edu

Abstract. Given a one-point algebraic geometry code, the Clifford defect is a rational number associated to the Weierstrass semigroup of such point describing the error-capability of the so-called Modified Algorithm. The Clifford defect also arises in other contexts involving decoding one-point codes. In this work, we study the Clifford defect for some numerical semigroups and give explicit formulas.

Introduction

Let $\mathcal{X}$ be an algebraic nonsingular absolutely irreducible curve over $\mathbb{F}_q$, $n+1$ rational points $P_1, \ldots, P_n, Q$ and $r \in \mathbb{N}$. The associated one-point code is defined as the following evaluation code:

$$C(P_1 + \ldots + P_n, rQ) := \{(f(P_1), f(P_2), \ldots, f(P_n)) \in \mathbb{F}_q^n : \ f \in \mathscr{L}(rQ)\}.$$

Under the assumption that $r < n$, the evaluation map $f \mapsto (f(P_1), \ldots, f(P_n))$ is injective and so the dimension of $C(P_1 + \ldots + P_n, rQ)$ is $k := \dim \mathscr{L}(rQ)$. The minimum distance d of the code can be proved to satisfy $d \geq n - k + 1 - g$, a kind of «lower Singleton bound» where g denotes the genus of the curve. This means that if we have a curve with a large number of rational points and low genus, we can construct a code with large length and large minimum distance. In fact, the existence of curves having an increasing number of rational points while maintaining such low genus was used to construct the first example of a family of codes beating the Gilbert-Varshamov bound, that is, a sequence of codes that asymptotically performs better than random codes.

Regarding the decoding process of these codes, several algorithms exist. One of them is the Modified Algorithm (MA), introduced in [6]. It works by computing an error locator and employing it for decoding up to half the minimum distance minus a defect in polynomial time. This defect is known as the Clifford defect and depends entirely on the Weierstrass semigroup associated to Q. The Weierstrass semigroup of $\mathcal{X}$ at Q is defined as

$$S := \{a \in \mathbb{N} : \ \mathscr{L}((a-1)Q) \neq \mathscr{L}(aQ)\}.$$

J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, V. Sotomayor (eds.): Proceedings of the XIX EACA, pp. 88-92 (2026).
ISBN: 978-84-09-87277-0

That is, S is the set of all $a \in \mathbb{N}$ such that there exists a function $f \in \mathbb{F}_q(\mathcal{X})$ with a unique pole at Q of order $\nu_Q(f) = -a$. It is known that S is a numerical semigroup whose number of gaps is the genus of $\mathcal{X}$ [7, Theorem 1.6.8]. In a previous work, the second and third authors showed how the Clifford defect can be used for designing algorithms for distributed matrix multiplication with good parameters. Also, the first and fourth authors made use of the Clifford defect in [1] in the context of fractional decoding of algebraic geometry codes

With this as a motivation, in this work we address the problem of giving explicit formulas for the Clifford defect for some families of numerical semigroups. We focus on numerical semigroups arising as the Weierstrass semigroup of curves that are commonly used in coding theory.

Basic properties

Let S be a numerical semigroup. Denote by $c := \max(\mathbb{N} \setminus S) + 1$ its conductor, by $g := |\mathbb{N} \setminus S|$ its genus (which coincides with the genus of the curve when S is a Weierstrass semigroup) and by $m := \min(S \setminus \{0\})$ its multiplicity. We define

$$\begin{aligned} \sigma : S \cap [0, c] &\to \mathbb{Q} \\ s &\mapsto \frac{s}{2} - |S \cap [0, s]| + 1. \end{aligned}$$

The Clifford defect is defined as the maximum of σ. The following simple lemma is useful for finding such maximum.

Lemma 1. *Let $s_1, s_2 \in S$ with $s_1 \leq s_2$. Then $\sigma(s_1) \leq \sigma(s_2)$ if and only if*

$$|S \cap [s_1 + 1, s_2]| \leq \frac{s_2 - s_1}{2},$$

with equality occurring if and only if $\sigma(s_1) = \sigma(s_2)$.

For instance, from the previous lemma it is easy to see that if $S \cap [0, c]$ has no two consecutive elements (such semigroups are called sparse), then σ is increasing and so the Clifford defect is attained at c. This easily solves the problem for semigroups arising from:

1. Hyperelliptic curves: $S = \langle 2, 2g + 1 \rangle$ so the Clifford defect is $\sigma(2g + 1) = \frac{1}{2}$.
2. The asymptotically optimal tower of function fields of García-Stichtenoth [5].

In fact, we can narrow the domain $S \cap [0, c]$ where to look for since σ will be always maximized at some $s \geq \frac{c}{2}$ as we showed in [2]. For symmetric semigroups, we have the following similar result that greatly simplifies computing the Clifford defect.

Theorem 2. *If S is symmetric, then σ attains its maximum at some $s \in S$ such that $g - \lceil \frac{m}{2} \rceil \leq s \leq g$. Moreover, if σ attains its maximum at $s \in S \cap [0, c]$, then $\sigma(s) = \sigma(c - s)$.*

The proof of the previous theorem follows essentially from the fact that, for a symmetric semigroup S, given $x \in [0, c - 1]$, we have that $x \in S$ if and only if $c - x - 1 \notin S$. The «only if» part is always true for an arbitrary semigroup, and the «if» part characterizes symmetric

semigroups. This property allows us to ensure that $\sigma(s) = \sigma(c-s-1) - \frac{1}{2}$ for every $s \in S \cap [0,c]$ and the upper bound follows easily since $g = \frac{c}{2}$ for symmetric semigroups. The lower bound requires some computations comparing $\sigma(s)$ and $\sigma(s+m)$ together with hypothesis of S being symmetric.

Explicit formulas

Computing both the Clifford defect of a semigroup and where it is attained is a problem that requires different approaches depending on the semigroup. Nevertheless, a common technique can be employed for some families of semigroups. Let us start considering the semigroups generated by a set of consecutive numbers $m, m+1, \dots, m+h$. We can obtain a sort of «parametrization» of the elements in $S \cap [0,c]$ in a way that is compatible with the usual order of $\mathbb{N}$ as the following shows.

Lemma 3 ([3, Lemma 1]). *Let $S = \langle m, m+1, \dots, m+h\rangle$ with $1 \leq h \leq m-1$. Then, $S = \{\lambda_1 m + \lambda_2 : 0 \leq \lambda_2 \leq h\lambda_1\}$. Moreover, given such λ_1, λ_2 and λ_1', λ_2', we have $\lambda_1 m + \lambda_2 \leq \lambda_1' m + \lambda_2'$ if and only if $(\lambda_1, \lambda_2) \preceq_{lex} (\lambda_1', \lambda_2')$, for $\lambda_1' m + \lambda_2' \leq c$.*

Using this description, we can compute explicit values of $|S \cap [0,s]|$ for a given $s \in S \cap [0,c]$, consequently obtaning an explicit formula for the Clifford defect.

Theorem 4 (Generated by an interval). *Let $S = \langle m, m+1, \dots, m+h\rangle$. Its Clifford defect is*

$$\sigma\left(\left\lceil \frac{m-2}{2h} \right\rceil m\right) = \left\lceil \frac{m-2}{2h} \right\rceil \left(\frac{m}{2} - 1\right) - h\left(\frac{\left\lceil \frac{m-2}{2h} \right\rceil}{2}\right).$$

This same idea can be applied to other families of semigroups: «parametrize» S while being compatible with its ordering and employ it to count elements under each $s \in S$. As in the case of numerical semigroups generated by an interval, this can yield explicit formulas for the Clifford defect. All the semigroups that we study in this section making use of this idea are known to be Weierstrass semigroups.

Theorem 5 (Klein curve). *Let $S = \langle m, 2m-1, 3m-2, \dots, (m-1)m - m + 1\rangle$. Its Clifford defect is*

$$\sigma(s) = \frac{1}{2}\left\lceil \frac{m-1}{2} \right\rceil \left(\left\lfloor \frac{m-1}{2} \right\rfloor + 1\right) - \frac{1}{2}.$$

where $s := \left\lceil \frac{m-1}{2} \right\rceil (m-1) + 1$.

Theorem 6 (A quotient of the Hermitian curve). *Let $S = \langle m, q\rangle$ where $q + 1 = mr$. Its Clifford defect is*

$$\sigma(s) = \begin{cases} \frac{1}{8}(m-1)(q-1) & \text{if } m \text{ is even,} \\ \frac{1}{8}(m-1)(q-r-1) & \text{if } m \text{ is odd.} \end{cases}$$

where $s := q\left(\left\lceil \frac{m}{2} \right\rceil - 1\right)$.

The next semigroup is one arising from the Pedersen-Sørensen curve. The question of computing the Clifford defect of this semigroup was studied in [4], where some bounds were given on its assymptotic behaviour. We obtain where σ is maximized and, for the family of curves known as Suzuki curve, a particular case of the Pedersen-Sørensen curve, we give explicit formulas for this maximum.

Theorem 7 (Pedersen-Sørensen curve)**.** *Let* $S = \langle q, q+q_0, q+tq_0, (t-1)q+tq_0+1\rangle$ *with* $q := tq_0^2$ *a power of a prime* p*. Its Clifford defect is attained at*

$$s := \begin{cases} g = \frac{tq_0(q-1)}{2} & \text{if } p \text{ is odd,} \\ g - \frac{q}{2} = \frac{(tq_0-1)(q-1)+1}{2} & \text{if } p \text{ even.} \end{cases}$$

If $t = 2$ *(Suzuki curve), the Clifford defect is* $\sigma(s) = \frac{q_0}{12}(4q - 3q_0 - 8)$.

There is one significant difference between the proofs of Theorems 4, 5 and 6 with respect to the proof of Theorem 7. In Theorems 4, 5 and 6, the authors were able to give a complete parametrization of $S \cap [0, c]$ in a similar way to Lemma 3. In contrast, for proving Theorem 7, only some elements of $S \cap [0, c]$ were parametrized, being this sufficient to assert where σ attains its maximum, but not enough to give an explicit formula for $|S \cap [0, s]|$ (s is defined in the statement of Theorem 7).

The last semigroup for which we compute the Clifford defect is one associated to the Norm-trace curve, a generalization of the Hermitian curve commonly studied in coding theory. We achieve a complete parametrization of $S \cap [0, c]$ and so we are able to give explicit formulas for the Clifford defect of this semigroup.

Theorem 8 (Norm-trace curve)**.** *Let* $S = \langle q^{r-1}, \frac{q^r-1}{q-1}\rangle$.

1. *If* q *is odd,* σ *is maximized at* g *and*

$$\sigma(g) = \begin{cases} \frac{1}{8(q-1)}(q^{2r-1} - 4q^r + 2q^{r-1} + q^2 + q - 1) & \text{if } r \text{ is even,} \\ \frac{1}{8(q-1)}(q^{2r-1} + q^{2r-4} - q^{2r-6} - 4q^r + 3q^{r-3} + q^2 + 3q - 4) & \text{if } r \text{ is odd.} \end{cases}$$

2. *If* q *is even,* σ *is maximized at* $g - \frac{q^{r-1}}{2}$ *and*

$$\sigma\left(g - \frac{q^{r-1}}{2}\right) = \frac{q}{8(q-1)}\left(q^{2r-2} - 4q^{r-1} + 2q^{r-2} + q\right).$$

Acknowledgements. The first and the fourth authors have been partially supported by NSF DMS-2201075 and the Commonwealth Cyber Initiative. The second and the third authors have been supported by Grant PID2022-138906NB-C21 funded by MICIU/AEI/10.13039/501100011033 and by ERDF/EU.

References

[1] E. Camps-Moreno, G.L. Matthews, W. Santos: Error correction from partial information via norm-trace codes. *IEEE International Symposium on Information Theory (ISIT)*, 2814–2819 (2024).

[2] A. Fidalgo-Díaz, U. Martínez-Peñas: Distributed matrix multiplication with straggler tolerance using algebraic function fields. *IEEE Trans. Inform. Theory* **71**(2), 996–1006 (2024).

[3] P.A. García-Sánchez, J.C. Rosales: Numerical semigroups generated by intervals. *Pacific J. Math.* **191**(1), 75–83 (1999).

[4] C. Kirfel: On the Clifford defect for special curves. *Proceedings of Arithmetic, geometry and coding theory (Luminy, 1993)*, 67–75 (1996).

[5] R. Pellikaan, H. Stichtenoth, F. Torres: Weierstrass semigroups in an asymptotically good tower of function fields. *Finite Fields Appl.* **4**(4), 381–392 (1998).

[6] A.N. Skorobogatov, S.G. Vladut: On the decoding of algebraic-geometric codes. *IEEE Trans. Inform. Theory* **36**(5), 1051–1060 (2002).

[7] H. Stichtenoth: *Algebraic function fields and codes*. Springer Berlin Heidelberg (2009).

Model invariants for the Equal Input model

M. Casanellas*, D. Deligeorgaki◇†, G. Dilaver‡, R. Homs*

◇ *Speaker at EACA 2026*

* *Universitat Politècnica de Catalunya*

† *Universitat de Barcelona*

‡ *Bursa Technical University*

marta.casanellas@upc.edu, deligeorgaki@ub.edu, gokcen.dilaver@btu.edu.tr, rhoms@crm.cat

Abstract. We derive phylogenetic invariants for the Equal Input (EI) model using the framework of Algebraic Time Reversible (ATR) models that was recently developed by Casanellas, Homs and Torres. Specifically, we state all linear (binomial and non-binomial) model equations for tripods with $\kappa \geq 3$ states and quartets with $\kappa \geq 4$ states. We also establish a large class of (binomial) linear equations that hold for any tree with n leaves, regardless of its topology, for $n \geq 3$ and κ states.

Introduction

Algebraic phylogenetics sits at the crossroads of algebra, geometry, statistics, and evolutionary biology and has seen steady growth over the past decades (see [2, 5], [11, Chapter 15]). At the heart of algebraic phylogenetics are phylogenetic invariants: polynomial equations that vanish on probability distributions arising from Markov models on phylogenetic trees. These distributions form an algebraic variety V_T for a given phylogenetic tree T, and the invariants are precisely the polynomials in its defining ideal $\mathcal{I}(V_T)$. Naturally, the structure of V_T depends on the biological constraints imposed on the Markov process, leading to different substitution models. Explicit phylogenetic invariants have been obtained for several equivariant models, a class of algebraically tractable models that includes group-based, strand-symmetric models, and general Markov models. In general, many equivariant models are either too simple for practical use or too parameter-rich to describe their phylogenetic invariants explicitly.

Algebraic time-reversible (ATR) models [1] provide a flexible and biologically meaningful class of substitution processes that overcome many of the limitations of general equivariant models. They include the GTR model [13] and TN93 [12]. ATR models are compatible with the continuous-time processes most commonly assumed in phylogenetic inference and admit a coherent algebraic treatment. Recently, Casanellas, Homs, and Torres [3] developed an algebraic framework for ATR models and illustrated these techniques in detail for TN93. Specifically, they computed the equations that cut out the corresponding phylogenetic variety on an open set when the underlying tree is a tripod (three leaves) or a quartet (four

J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, V. Sotomayor (eds.): Proceedings of the XIX EACA, pp. 93-97 (2026).
ISBN: 978-84-09-87277-0

leaves). Subsequently, in [8], Casanellas, Garbett, Homs, Korchmaros and Paul computed phylogenetic invariants for F81 [6] and F84 [7], two submodels of TN93. They generalize the JC69 [9] and Kimura 2-parameter [10], respectively, to an arbitrary stationary distribution, thus constituting examples of algebraically tractable, non-equivariant models.

All the above models (TN93, F81 and F84) are nucleotide substitution models, which mathematically means that they admit 4 states (corresponding to nucleotides). In general, phylogenetic models are often defined to allow any number of states κ, with a particular interest in the cases $\kappa = 4$ and $\kappa = 20$; the latter corresponds to amino acid substitution in protein sequences. The models that are of interest for nucleotide substitution are different from those for amino acid substitution. The generalization of F81 for any number of states is the simplest model of interest for amino acid substitution that does not have a uniform distribution. It is the Equal Input model (EI), where the name comes from equalities in transition matrices in the corresponding Markov process. Specifically, for any edge e of T,

$$M_e = \begin{pmatrix} 1 - a\pi_{2:\kappa} & a\pi_2 & \dots & a\pi_\kappa \\ a\pi_1 & 1 - a(\pi_1 + \pi_{3:\kappa}) & \dots & a\pi_\kappa \\ \vdots & \vdots & \ddots & \vdots \\ a\pi_1 & a\pi_2 & \dots & 1 - a\pi_{1:(\kappa-1)} \end{pmatrix}, \tag{1}$$

where a depends on e. Casanellas and Steel [4] described the structure and dimension of the phylogenetic varieties of EI models for any number of states and any number of leaves. They gave precise descriptions of the equations that cut out the model in the case of 4 leaves, which however are quite complex to put to use.

In this extended abstract, we derive phylogenetic invariants for EI models using the framework of ATR models from [3]. We perform a change of basis that simplifies the equations, using which we state all linear phylogenetic equations for tripods and quartets. Linear invariants that hold for any tree topology (model equations) are important because they describe the space of distributions that can arise from mixtures of evolutionary processes on n-leaf trees and provide a way to guide model selection. We also establish a large class of model equations that cut out V_T for any tree T evolving under the EI model.

Preliminaries

We present some of the definitions below. For the technical details we point the reader to [3] and [8] (co-authored by the first and last author of this extended abstract).

Definition 1. Let $\pi \in \Delta^\circ_{\kappa-1}$ be a distribution in the standard open simplex of dimension $\kappa - 1$, and let $B = \{u^1 = \pi, u^2, \dots, u^\kappa\}$ be a π-orthogonal basis in $\mathbb{R}^\kappa$. A phylogenetic tree T *evolves under a* B*-time-reversible model* if

- the Markov matrices M^e, for each edge $e \in E(T)$ (on the Markov process on T) all have B as a left eigenbasis,
- $\pi^r = \pi$ (stationary distribution at the root).

Let A be the change-of-basis matrix from B to the standard basis and consider $\Lambda^e = A^{-t}M^eA^{-1}$, $e \in E(T)$. We parametrize a B-time-reversible model for n-leaf tree T as:

$$\begin{array}{ccc} \prod_{e\in E(T)} \mathbb{C}^\kappa & \xrightarrow{\varphi_T} & \bigotimes^n \mathbb{C}^\kappa \\ (\Lambda^e)_{e\in E(T)} & \mapsto & \sum_{i_1,\dots,i_n} \bar{p}^T_{i_1\dots i_n} u^{i_1} \otimes \cdots \otimes u^{i_n}. \end{array}$$

When all $\Lambda^e = Id$, we call the tensor the no evolution point, denoted $\bar{p}^0 = \varphi_T(\{Id\}_{e\in E(T)})$.

We denote by $I(E)$ the interior edges and by $P(E)$ the pendant edges (edges adjacent to leaves). We use

$$\bar{q} = \varphi_T(\{Id\}_{e\in P(E)}; \{\Lambda^e\}_{e\in I(E)})$$

when we assume the identity transition matrix on all pendant edges. If all transition matrices are generic diagonal matrices, we use $\bar{p} = \varphi_T(\{\Lambda^e\}_{e\in E(T)})$. Observe that, if $P(E) = \{e_1, \dots, e_n\}$, and $\lambda^{e_j}_{i_j}$ are eigenvalues,

$$\bar{p} = (\Lambda^{e_1}, \dots, \Lambda^{e_n}) \cdot \bar{q}, \quad \text{i.e., } \bar{p}_{i_1\dots i_n} = \lambda^{e_1}_{i_1} \dots \lambda^{e_n}_{i_n} \bar{q}_{i_1\dots i_n}.$$

Finally, when we rescale the parametrization via the no evolution point to obtain monic expressions on the eigenvalues for monomial coordinates, we use the following. If $\bar{p}^0_{i_1\dots i_n} \neq 0$,

$$\tilde{p}_{i_1\dots i_n} = \frac{\bar{p}_{i_1\dots i_n}}{\bar{p}^0_{i_1\dots i_n}}, \quad \tilde{q}_{i_1\dots i_n} = \frac{\bar{q}_{i_1\dots i_n}}{\bar{p}^0_{i_1\dots i_n}}.$$

Otherwise, $\bar{p}_{i_1\dots i_n} = \tilde{p}_{i_1\dots i_n}$. Similarly, one obtains $\tilde{p}_{i_1\dots i_n} = \lambda^{e_1}_{i_1} \dots \lambda^{e_n}_{i_n} \tilde{q}_{i_1\dots i_n}$.

A π-orthogonal basis for EI on κ states

Consider $\pi = (\pi_1, \dots, \pi_\kappa)$ a distribution on κ states with nonzero coordinates. Let $\pi_{1:j}$ be the sum $\pi_1 + \cdots + \pi_j$. Also, let $u^1 = \pi^t$ and for $j = 2, \dots, \kappa$ let u^j be the vector whose coordinates are

$$u^j_i = \begin{cases} 0, & \text{if} \quad i > \kappa + 2 - j \\ \pi_i, & \text{if} \quad i < \kappa + 2 - j, \\ -\pi_{12:(i-1)}, & \text{if} \quad i = \kappa + 2 - j. \end{cases}.$$

Proposition 2. *The collection of vectors $B = \{u^1, \dots, u^\kappa\}$ is a π-orthogonal basis and the EI model on κ states is a B-time-reversible model.*

Proof sketch. For any edge e, the transition matrix is M_e given in (1) has eigenvalues $\lambda_1 = 1$ (multiplicity 1) and $\lambda_2 = 1 - a$ (multiplicity $\kappa - 1$), with the eigenspaces of λ_1, λ_2 spanned by $u^1, u^2, \dots, u^\kappa$, respectively. Hence each $u^i \in B$ is a left-eigenvector of M_e, and B is a π-orthogonal eigenbasis for all edges.

The vectors $u_2, \dots, u_\kappa$ are linearly independent and their entries some to 0, hence $\langle u_1, u_j\rangle_\pi = 0$. Moreover, for $1 < j < l \leq \kappa$, a direct computation gives $\langle u_j, u_l\rangle_\pi = 0$. Hence, the vectors in B form a π-orthogonal basis. □

Results

Tripods

The model equations of the EI model on a tripod for $\kappa \geq 3$ are:

(a) $\tilde{p}_{abc} = \tilde{p}_{def}$ where $1 < a, b, c, d, e, f \leq \kappa$; (b) $\tilde{p}_{1\kappa\kappa}\tilde{p}_{\kappa 1\kappa}\tilde{p}_{\kappa\kappa 1} - \tilde{p}_{111}\tilde{p}^2_{\kappa\kappa\kappa} = 0$;
(c) $\tilde{p}_{abc} = 0$ where wlog $1 \leq a, b < c \leq \kappa$; (d) $\tilde{p}_{122} = \cdots = \tilde{p}_{1\kappa\kappa}$ (up to symmetry);

Quartets

The *symmetry* equations of the EI model on a quartet, $\kappa \geq 4$, are:

(a) $\tilde{p}_{i_1 i_2 i_3 i_4} = 0$ when $\max\{i_1, i_2, i_3, i_4\}$ is unique; (b) tripod equations $\tilde{p}_{i_1 i_2 i_3 1} = \tilde{p}_{j_1 j_2 j_3 1}$;
(c) $\tilde{p}_{aabb} = \tilde{p}_{bbaa}$ (up to symmetry), $1 < a, b \leq \kappa$; (d) $\tilde{p}_{i_1 i_2 i_3 i_4} = \tilde{p}_{j_1 j_2 j_3 j_4}$ if $\max\{i_1, i_2, i_3, i_4\}$ is attained 2 or 3 times and $\min\{i_1, i_2, i_3, i_4\}$ only once for $1 < i_s \leq \kappa$ (and same for j's).

Non-binomial model equations are also computed for $\kappa \geq 4$.

Trees with n leaves

Let T be an n-leaf phylogenetic tree evolving under an EI model. We show:

$$\tilde{p}_{i_1 \ldots i_n} = 0 \quad \Longleftrightarrow \quad \text{unique } \max\{i_1, i_2, \ldots, i_n\}.$$

Moreover, $\tilde{p}_{i_1 i_2 \ldots i_n} = \tilde{p}_{j_1 j_2 \ldots j_n}$ whenever $\#\max\{i_1, \ldots, i_n\} = 2, 3$, and other values occur at most once (similarly for j's), $1 < i_s, j_s \leq \kappa \geq n$. For example, $\tilde{p}_{23455} = \tilde{p}_{35666}$.

If $\mathbf{i} = i_1 \ldots i_n$ is a state pattern at the set of leaves of a tree T, $L(T)$, we call $\rho(\mathbf{i}) = P_1|P_2|\ldots|P_m$ the partition it induces on the set of leaves of T, $L(T)$. That is, leaves m and k belong to the same component P_s of the partition $\rho(\mathbf{i})$ if $i_m = i_k$. Let NZ be the set of state patterns whose maximum is attained at least twice (nonzero case). We compute the following large class of symmetry equations for V_T.

Theorem 3. *Suppose that* $\mathbf{i} = i_1 \ldots i_n$ *and* $\mathbf{j} = j_1 \ldots j_n$ *are two state patterns at* $L(T)$ *that lie in* NZ*, for an* n*-leaf tree with* $\kappa \geq 4$ *states, and*

(1) $\rho(\mathbf{i}) = \rho(\mathbf{j})$,
(2) $i_l = j_l$ *if* l *is not a singleton in* $\rho(\mathbf{i})$,
(3) if l *singleton in* $\rho(\mathbf{i})$ *then* $i_l \neq 1$, $j_l \neq 1$. *Moreover,* $i_a < i_l < i_b$ *if and only if* $j_a < j_l < j_b$ *for any two leaves* a, b.

Then $\tilde{p}_{i_1 \ldots i_n} = \tilde{p}_{j_1 \ldots j_n}$.

The proof is by induction, using the gluing theorem from [3]. [4] provides the number of equations that cut out V_T. Even though we do not identify them all, the striking simplicity of the expressions above shows why our approach through a change of basis is worth-while.

References

[1] E.S. Allman, J.A. Rhodes: Phylogenetic invariants for stationary base composition. *J. Symbolic Comput.* **41**(2), 138–150 (2006).

[2] E.S. Allman, J.A. Rhodes: *Phylogenetic invariants*. Reconstructing evolution: New mathematical and computational advances, O. Gascuel (ed.), Oxford University Press, 108–146 (2007).

[3] M. Casanellas, R. Homs, A. Torres: A novel algebraic approach to time-reversible evolutionary models. *SIAM J. Appl. Math.* **84**(4), 1845–1867 (2024).

[4] M. Casanellas, M. Steel: Phylogenetic mixtures and linear invariants for equal input models. *J. Math. Biol.* **74**(5), 1107–1138 (2016).

[5] N. Eriksson, K. Ranestad, B. Sturmfels, S. Sullivan: Phylogenetic algebraic geometry. *Projective Varieties with Unexpected Properties*, Walter de Gruyter, 237–256 (2005).

[6] J. Felsenstein: Evolutionary trees from DNA sequences: A maximum likelihood approach. *J. Mol. Evol.* **17**(6), 368–376 (1981).

[7] J. Felsenstein, G.A. Churchill: A hidden Markov model approach to variation among sites in rate of evolution. *Mol. Biol. Evol.* **13**(1), 93–104 (1996).

[8] R. Homs, M. Casanellas, J. Garbett, A. Korchmaros, N. Paul: Computing phylogenetic invariants for time-reversible models: from TN93 to its submodels. *ArXiv:2505.20526* (2025).

[9] T.H. Jukes, C.R. Cantor: *Evolution of protein molecules*. Mammalian Protein Metabolism, H.N. Munro (ed.), Academic Press, 21–132 (1969).

[10] M. Kimura: A simple method for estimating evolutionary rates of base substitutions through comparative studies of nucleotide sequences. *J. Mol. Evol.* **16**(2), 111–120 (1980).

[11] S. Sullivant: *Algebraic statistics*. Graduate Studies in Mathematics **194**, American Mathematical Society (2018).

[12] K. Tamura, M. Nei: Estimation of the number of nucleotide substitutions in the control region of mitochondrial DNA in humans and chimpanzees. *Mol. Biol. Evol.* **10**(3), 512–526 (1993).

[13] S. Tavaré: Some probabilistic and statistical problems on the analysis of DNA sequences. *Lect. Math. Life Sci.* **17**, 57–86 (1986).

Phylogenetic networks evolving under G-equivariant models

M. Casanellas Rius*, J. Fernández-Sánchez◇*, E. Gross†, B. Hollering‡, S. Sullivant≀

◇ *Speaker at EACA 2026*

* *Universitat Politècnica de Catalunya*

† *University of Hawai'i*

‡ *Max Planck Institute for Mathematics in the Sciences*

≀ *North Carolina State University*

marta.casanellas@upc.edu, jesus.fernandez.sanchez@upc.edu, egross@hawaii.edu, benjamin.hollering@mis.mpg.de, smsulli2@ncsu.edu

Abstract. We study the identifiability of level-1 networks within the framework of G-equivariant models. This family comprises a wide and natural class of Markov models on trees and networks, defined by the action of a permutation group G on the state space together with the condition that both the transition matrices and the stationary distributions are invariant under this action. Several well-known models in molecular phylogenetics–such as the Jukes-Cantor model, the Kimura 2-parameter and 3-parameter models, the strand symmetric model, and the general Markov model–can be viewed as particular instances of G-equivariant models.

Introduction

Phylogenetic networks extend phylogenetic trees to model reticulate evolutionary events such as hybridization and horizontal gene transfer. Among them, level-1 networks–where reticulation cycles are pairwise disjoint–form a simple yet expressive class that retains much of the tree structure while allowing limited non-tree behavior.

A key issue in phylogenetic modeling is *identifiability*: whether the network topology can be recovered, in principle, from the joint distribution of character states observed at the leaves. Identifiability under various models has been studied for level-1 networks, including group-based Markov models [GL18, HS21, GvIJ+21].

In this work, we investigate identifiability of level-1 networks under G-equivariant models, a broad class of Markov models defined by invariance under a permutation group action. Many standard models in molecular phylogenetics arise as special cases. We derive distinguishing equations based on rank conditions of flattening matrices associated with distribution tensors, providing tools to prove that certain networks are distinguishable.

J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, V. Sotomayor (eds.): Proceedings of the XIX EACA, pp. 98-102 (2026).
ISBN: 978-84-09-87277-0

Preliminaries

Σ denotes a set of *states* and we call $\kappa \geq 2$ its cardinal. W is the $\mathbb{C}$-vector space of dimension κ where we identify the standard basis with the elements of Σ.

Equivariant models

If $G < \mathfrak{S}_\kappa$ is a permutation group acting on Σ, the G-equivariant substitution model considers only distributions that invariant and transition matrices that are equivariant under the action of G (see [DK09] for further details).

The action of G in Σ extends linearly to the permutation representation of the linear space W spanned by the elements in Σ. Equivariant models provide a wide family of examples of algebraic evolutionary models: if $\kappa = 4$ and we identify the states of the model with the set of nucleotides, the Jukes-Cantor model, the Kimura models with 2 or 3 parameters, the strand symmetric model or the general Markov model are instances of equivariant models. The models in this list have been largely studied in the literature (see [DK09] or [CFS11]).

For any $l \in \mathbb{N}$, the natural representation in $\otimes^l W$ induced by the permutation representation and write $(\otimes^l W)^G$ for the variety of G-invariant tensors. This induces a decomposition of $\otimes^l W$ into isotypic components (Maschke's theorem), where each component is naturally associated with one irreducible representation of G.

Networks

We adopt the terminology of [GvIJ+21] and consider *binary phylogenetic level-1 tree-child networks*. For $k \geq 3$, a k-*sunlet* is a k-leaf network with a single reticulation node of maximal length equal to k. If $\mathcal{N}$ is an n-leaf phylogenetic network with r reticulation vertices, each binary vector $\sigma \in \{0,1\}^r$ encodes the possible choices for the reticulation edges and results in an n-leaf tree T_σ (these are the *displayed trees* of $\mathcal{N}$).

We consider a distribution π at the root ρ and associate a $\kappa \times \kappa$ transition matrix from a substitution model to each directed edge of $\mathcal{N}$. For $1 \leq i \leq r$, δ_i represents the probability that a particular site was inherited along the edge e_i^1. The collection of parameters is denoted as θ and we call θ_σ the restriction of θ to the tree T_σ. We can then define a distribution on n-tuples of states in Σ at the leaves of the network as

$$\varphi_{\mathcal{N}}(\theta) = \sum_{\sigma \in \{0,1\}^r} \left(\prod_{i=1}^{r} \delta_i^{1-\sigma_i} (1-\delta_i)^{\sigma_i} \right) \varphi_{T_\sigma}(\theta_\sigma).$$

where $\varphi_{T_\sigma}(\theta_\sigma)$ is the parameterization of the displayed tree T_σ. By letting $\Theta_{\mathcal{N}}$ be $= \mathbb{C}^m \times W \times \prod_{e \in E(\mathcal{N})} \mathbb{M}$, this defines a polynomial map $\varphi_{\mathcal{N}} : \Theta_{\mathcal{N}} \longrightarrow \otimes^n W$, which parametrizes the algebraic variety $V_{\mathcal{N}} = \overline{\mathrm{Im}\,(\varphi_{\mathcal{N}})}$ inside $\mathbb{L}_n$. Similarly, for a given permutation group G, we can restrict the parameterization above to the G-equivariant parameters $\Theta_{\mathcal{N}}^G$. We will denote the Zariski closure of the image of this restriction by $V_{\mathcal{N}}^G = \overline{\mathrm{Im}\,\varphi_{\mathcal{N}}^G} \subseteq \mathbb{L}_n^G$. The elements of the ideal of this variety are referred to in the literature as *phylogenetic invariants*. The parameters of this model are $\mathcal{N}$ and the stochastic parameters in $\Theta_{\mathcal{N}}^G$.

Identifiability and Distinguishability

Definition 1. Two network models $\mathcal{M}^G_{\mathcal{N}_1}, \mathcal{M}^G_{\mathcal{N}_2}$ are *distinguishable* if the set of stochastic parameters in each parameter space that provide distributions compatibles with the other model is a set of Lebesgue measure zero. If this only occur for one of the models but not necessarily for both, we say that the models are *weakly distinguishable*.

The network models $\mathcal{M}^G_{\mathcal{N}_1}, \mathcal{M}^G_{\mathcal{N}_2}$ are *algebraically distinguishable* if $V^G_{\mathcal{N}_1} \cap V^G_{\mathcal{N}_2}$ is a proper subvariety of $V^G_{\mathcal{N}_1}$ and of $V^G_{\mathcal{N}_2}$. They are *weakly algebraically distinguishable* if $V^G_{\mathcal{N}_1} \neq V^G_{\mathcal{N}_2}$.

Definition 2. Let $\mathcal{C}^G_N = \{\mathcal{M}^G_{\mathcal{N}}\}_{\mathcal{N}\in N}$ be a class of phylogenetic network models. The network parameter is *(weakly) generically identifiable within* $\mathcal{C}^G_N$ if any two network models in $\mathcal{C}^G_N$ are (weakly) distinguishable.

Let $A|B$ be a bipartition of L. If $P \in \otimes^n W$, the *flattening* $flat_{A|B}(P)$ of P is the $\kappa^{|A|} \times \kappa^{|B|}$-matrix whose (x_A, x_B) entry is the coordinate of P that has states x_A at the indices in A and x_B at the indices in B. By [AR08, SFB23], if T is a phylogenetic tree and $P = \varphi_T(\theta)$ for generic $\theta \in \Theta$, then rank $flat_{A|B}(P) = \kappa^{\ell_T(A|B)}$, where $\ell_T(A|B)$ is the parsimony score of $A|B$ in T. This result was generalized for equivariant models by using representation theory. In this case, the matrix has a block-diagonal structure in terms of the irreducible representations of the group G, and the condition translates into rank constraints for the blocks (see [DK09, CFS11] for details).

Dimension and Reparameterization

It is helpful to reparametrize the varieties of networks with fewer parameters: $f^G_{\mathcal{N}} : \tilde{\Theta}^G_{\mathcal{N}} \to \mathbb{L}^G$. These new parameters are defined in terms of tensors spaces attached to each reticulation node. These tensors are defined as follows: consider the linear variety $\mathbb{E}^G \subset (\otimes^3 W)^G$ of tensors satisfying $t_{x,j,k} - t_{x,j',k} = t_{x,j,k'} - t_{x,j',k'} \quad \forall x, j, j', k, k' \in [\kappa]$, and $\sum_{x\in\Sigma} t_{x,j,k} = 1$. The idea is that such tensors represent the free parameters involved in the reticulation node.

Proposition 3. $\mathrm{Im}\,(f^G_{\mathcal{N}}) = \mathrm{Im}\,(\varphi^G_{\mathcal{N}})$. *In particular,* $V^G_{\mathcal{N}} = \overline{\mathrm{Im}\,(f^G_{\mathcal{N}})}$.

We derive the following formulas for the dimension of a level-1 phylogenetic network.

Theorem 4. *Let $\mathcal{N}$ be a binary level-1 network with n leaves, r reticulations, c_3 triangles, and c_4 four-cycles. Then, the dimension of the phylogenetic network model for the standard equivariant models are the following: GM(4):* $24n - 33 + 21r$*; SS:* $12n - 17 + 11r - c_3$*; K3P:* $6n - 9 + 6r - c_3$*; K2P:* $4n - 6 + 4r - c_3$ *and JC:* $2n - 3 + 2r - c_3$.

From this, the generic identifiability of the continuous parameters of the map $f^G_{\mathcal{N}}$ follows.

Identifiability of networks from rank conditions

Given a bipartition $A|B$ of the leaves $L(\mathcal{N})$, define $\varepsilon_{\mathcal{N}}(A|B)$ as the minimum cardinality of a set of edges $\{e_1, \ldots, e_s\} \subset E(\mathcal{N})$ such that every path from A to B contains at least

one edge of the set. Similarly, the *upper parsimony score* of $A|B$ relative to $\mathcal{N}$ is $l_{\mathcal{N}}(A|B) = \max\{l_T(A|B) \mid \mathcal{T} \text{ is displayed in } \mathcal{N}\}$, where $l_T(A|B)$ is the parsimony score of $A|B$ on $\mathcal{T}$. In general, we always have $\varepsilon_{\mathcal{N}}(A|B) \geq \ell_{\mathcal{N}}(A|B)$.

Theorem 5. *Let $\mathcal{N}$ be a phylogenetic network and $P \in \operatorname{Im} \varphi^{\mathcal{N}}$.*

(a) If $A|B$ is a bipartition of $L(\mathcal{N})$, then $\kappa^{\ell_{\mathcal{N}}(A|B)} \leq \operatorname{rank} flat_{A|B}(P) \leq \kappa^{\varepsilon_{\mathcal{N}}(A|B)}$.
(b) If P evolves under a G-model, the rank of the blocks of $Tf_{A|B}(P)$ are bounded by certain multiplicities attached to the irreducible representations of the group G.

Sufficient conditions for identifiability of level-1 networks

The following theorem now distills verifying identifibility for a specific G-equivariant model into checking a few number of conditions that can be confirmed computationally.

Theorem 6. *Fix a G-equivariant model of evolution on $\kappa \geq 3$ states, and consider the class $\mathcal{C}_{n,k}$ of level-one networks that includes all binary trees on n leaves and all binary level-1 network models on n-leaves where every cycle has length at least k. Assume that*

(H1) if $k \geq 4$, then any two sunlets of size k with the same reticulation leaf are distinguishable,
(H2) if $k = 3$, any two different 3-sunlets are distinguishable and any two 4-sunlets with the same reticulation leaf are distinguishable.

Then the network parameter is weakly generically identifiable with respect to $\mathcal{C}_{n,k}$.

After Theorem 6, we can establish identifiability for level-one networks with cycles of length at least six. For these networks, to establish identifiability it is enough to use the rank conditions on flattenings from Theorem 5.

Acknowledgements. The first two authors were partially supported by the project reference PID2023-146936NB-I00 financed by AQ1 the Spanish State Agency MCIN/AEI/10.13039/501100011033/ FEDER, UE, by the Severo Ochoa and María de Maeztu Program for Centers and Units of Excellence in R&D (project CEX2020-001084-M), and by the AGAUR project 2021 SGR 00603 Geometry of Manifolds and Applications, GEOMVAP.

References

[AR08] E.S. Allman, J.A. Rhodes: Phylogenetic ideals and varieties for the general Markov model. *Adv. Appl. Math.* **40**(2), 127–148 (2008).

[CFS11] M. Casanellas, J. Fernández-Sánchez: Relevant phylogenetic invariants of evolutionary models. *J. Math. Pures Appl.* **96**(3), 207–229 (2011).

[DK09] J. Draisma, J. Kuttler: On the ideals of equivariant tree models. *Math. Ann.* **344**(3), 619–644 (2009).

[GL18] E. Gross, C. Long: Distinguishing phylogenetic networks. *SIAM J. Appl. Algebra Geom.* **2**(1), 72–93 (2018).

[GvIJ+21] E. Gross, L. van Iersel, R. Janssen, M. Jones, C. Long, Y. Murakami: Distinguishing level-1 phylogenetic networks on the basis of data generated by Markov processes. *J. Math. Biol.* **83**, 32 (2021).

[HS21] B. Hollering, S. Sullivant: Identifiability in phylogenetics using algebraic matroids. *J. Symbolic Comput.* **104**, 142–158 (2021).

[SFB23] J. Snyman, C. Fox, D. Bryant: Parsimony and the rank of a flattening matrix. *J. Math. Biol.* **86** (2023).

The Hilbert polynomial of a filiform Lie algebra

M. Ceballos*, F.J. Castro-Jiménez◇†

◇ *Speaker at EACA 2026*

* *Universidad Loyola Andalucía*

† *Universidad de Sevilla*

mceballos@uloyola.es, castro@us.es

Abstract. With a complex finite-dimensional filiform Lie algebra $\mathfrak{g}$, we associate its bivariate Hilbert polynomial with respect to the bifiltration of the bracket ideals $[C^k\mathfrak{g}, C^\ell\mathfrak{g}]$. We give examples proving that the Hilbert polynomial can distinguish isomorphism classes of filiform Lie algebras that cannot be distinguished by other invariants.

Introduction

For a complex Lie algebra $\mathfrak{g}$, with Lie bracket $[\,,]$, and an integer $k \geq 1$, we denote by $C^k\mathfrak{g}$ the k-th ideal in the *lower central series* of $\mathfrak{g}$, i.e. $C^1\mathfrak{g} = \mathfrak{g}$ and $C^k\mathfrak{g} = [C^{k-1}\mathfrak{g}, \mathfrak{g}]$ for $k \geq 2$. One has $[C^k\mathfrak{g}, C^\ell\mathfrak{g}] \subseteq C^{k+\ell}\mathfrak{g}$ for $k, \ell \in \mathbb{N}$, $k, \ell \geq 1$ and the family of *bracket ideals* $[C^k\mathfrak{g}, C^\ell\mathfrak{g}]$ is called the *bracket bifiltration* of $\mathfrak{g}$. This bifiltration is indexed by the semigroup $\mathbb{Z}_{\geq 1} \times \mathbb{Z}_{\geq 1}$; see the first section.

A Lie algebra $\mathfrak{g}$ is said to be *filiform* ([7, III.1], [8, Sect. 1.5]) if $\mathfrak{g}$ has finite dimension $n \geq 2$ and $\dim(C^k\mathfrak{g}) = n - k$ for $k = 2, \ldots, n$. In particular, any filiform Lie algebra is nilpotent, and its nilpotency class equals its dimension.

A basic notion in this subject is that of *adapted basis* for a filiform Lie algebra. A basis $\{e_1, \ldots, e_n\}$ of a filiform Lie algebra $\mathfrak{g}$ is called *adapted*, see [7, III.2], [8, Sec. 4.2], if the following relations hold:

$$\begin{array}{ll} [e_1, e_h] = e_{h-1} & \text{for } 3 \leq h \leq n, \\ [e_2, e_h] = 0 & \text{for } 1 \leq h \leq n, \\ [e_3, e_h] = 0 & \text{for } 2 \leq h \leq n. \end{array}$$

As proved in *loc. cit.* any filiform Lie algebra admits an adapted basis.

We also use two numerical invariants, introduced in [2]. The first numerical invariant $z_1 = z_1(\mathfrak{g})$ is defined as

$$z_1 = \max\{k \in \mathbb{N} \,|\, C_{\mathfrak{g}}(C^{n-k+2}\mathfrak{g}) \supsetneq C^2\mathfrak{g}\}$$

where $C_{\mathfrak{g}}(\mathfrak{h})$ is the centralizer of a given Lie subalgebra $\mathfrak{h}$ of $\mathfrak{g}$, that is, the set of elements in $\mathfrak{g}$ whose bracket with any element of $\mathfrak{h}$ is zero. The invariant $z_2 = z_2(\mathfrak{g})$ is defined as

$$z_2 = \max\{k \in \mathbb{N} \,|\, C^{n-k+1}\mathfrak{g} \text{ is abelian}\}.$$

J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, V. Sotomayor (eds.): Proceedings of the XIX EACA, pp. 103-107 (2026).
ISBN: 978-84-09-87277-0

By definition, $C^{n-z_2+1}\mathfrak{g}$ is the largest abelian ideal in the lower central series of $\mathfrak{g}$. These two invariants satisfy the following relations, see [2, Th. 15]:

$$4 \leq z_1 \leq z_2 < n \leq 2z_2 - 2.$$

Given a n-dimensional non–model filiform Lie algebra $\mathfrak{g}$, we use the triple (z_1, z_2, n) to summarize the information about both invariants and the dimension of $\mathfrak{g}$. We say that (z_1, z_2, n) is the triple associated with $\mathfrak{g}$. Algebras with different triples are non–isomorphic. If one fixes an adapted basis $\{e_1, \ldots, e_n\}$ of $\mathfrak{g}$ then one has

$$z_1 = \min\{k \geq 4 \,|\, [e_k, e_n] \neq 0\}, \quad z_2 = \min\{k \geq 4 \,|\, [e_k, e_{k+1}] \neq 0\}.$$

Moreover, with respect to an adapted basis, the ideals of the lower central series are given by $C^1\,\mathfrak{g} = \mathfrak{g}$ and $C^k\mathfrak{g}$ is the $\mathbb{C}$–vector space generated by $\{e_2, \ldots, e_{n-k+1}\}$ where $2 \leq k \leq n-1$. This is proved in [7, III.2. Prop.].

In the second section we compute the Hilbert polynomials of the family of filiform Lie algebras of dimension 10 with $z_2 = 7$ and $z_1 = 5$. We show that the Hilbert polynomial distinguishes 6 isomorphism classes in the family. Certain computations have been performed using computer algebra systems `Maple`, [6] and `Macaulay2`, [4]. For basic concepts and the usual notation on Lie algebras, we have followed [5].

Bracket bifiltration and Hilbert polynomial

Let $\mathfrak{S}$ be the semigroup $\mathbb{Z}_{\geq 1} \times \mathbb{Z}_{\geq 1}$ endowed with its usual partial ordering $\preceq$. If $\mathfrak{g}$ is a Lie algebra, we denote by $F_{(\bullet,\bullet)}(\mathfrak{g})$, or simply $F_{(\bullet,\bullet)}$, the *bracket bifiltration* on $\mathfrak{g}$ indexed by $\mathfrak{S}$. That is, $F_{(k,\ell)} = F_{(k,\ell)}(\mathfrak{g}) := [C^k\mathfrak{g}, C^\ell\mathfrak{g}]$ where $(k,\ell) \in \mathfrak{S}$. The bracket bifiltration decreases in the sense that one has $F_{(k',\ell')} \subseteq F_{(k,\ell)}$ whenever $(k,\ell) \preceq (k',\ell')$.

Definition 1. If $\mathfrak{g}$ is a nilpotent Lie algebra of finite dimension, the Hilbert polynomial of $\mathfrak{g}$ is the bivariate polynomial associated with the bracket bifiltration of $\mathfrak{g}$, that is, the symmetric polynomial

$$\mathsf{HP}_\mathfrak{g} = \mathsf{HP}_\mathfrak{g}(t,s) := \sum_{k\geq 1, \ell \geq 1} \dim\,[C^k\mathfrak{g}, C^\ell\mathfrak{g}]\, t^k\, s^\ell \in \mathbb{Z}[t,s].$$

From now on, $\mathfrak{g}$ is a filiform Lie algebra of dimension $n \geq 2$. Then one has

$$\mathsf{HP}_\mathfrak{g} = (n-2)ts + \sum_{2\leq k\leq n-2} (n-k-1)(t^k\, s + t\, s^k) + \sum_{k\geq 2, \ell \geq 2} \dim\,[C^k\mathfrak{g}, C^\ell\mathfrak{g}]\, t^k\, s^\ell.$$

We also denote

$$\mathsf{HP}^{(0)}_\mathfrak{g} = \mathsf{HP}^{(0)}_\mathfrak{g}(t,s) = (n-2)ts + \sum_{2\leq k\leq n-2} (n-k-1)(t^k\, s + t\, s^k).$$

The degree of $\mathsf{HP}_\mathfrak{g}$ is $n-1$. We denote $\mathsf{hp}_{\mathfrak{g},k,\ell} = \dim\,[C^k\mathfrak{g}, C^\ell\mathfrak{g}]$ the coefficient of the monomial $t^k s^\ell$ of the Hilbert polynomial $\mathsf{HP}_\mathfrak{g}$. We write

$$\mathsf{HP}^{(2)}_\mathfrak{g} = \mathsf{HP}_\mathfrak{g} - \mathsf{HP}^{(0)}_\mathfrak{g}.$$

The super-index 2 indicates that the non-zero monomials in $\mathrm{HP}_{\mathfrak{g}}^{(2)}$ have degree ≥ 2. If $r \in \mathbb{R}$, we denote $r^* = n + 1 - r$.

Lemma 2. ([1, Lemma 1]) *With previous notations one has that* $\mathrm{hp}_{\mathfrak{g},k',\ell'} \leq \mathrm{hp}_{\mathfrak{g},k,\ell}$ *whenever* $(k,\ell) \preceq (k',\ell')$ *where* $\preceq$ *is the natural partial ordering in* $\mathfrak{S}$. *Moreover,*

$$[C^{z_2^*}\mathfrak{g}, C^{z_2^*}\mathfrak{g}] = \{0\}; \quad [C^k\mathfrak{g}, C^k\mathfrak{g}] = [C^k\mathfrak{g}, C^{k+1}\mathfrak{g}], \quad \text{for } k \geq 2$$

and then the coefficients of the three monomials $t^k s^k$, $t^{k+1}s^k$, $t^k s^{k+1}$ *in* $\mathrm{HP}_{\mathfrak{g}}$ *are identical, that is,* $\mathrm{hp}_{\mathfrak{g},k,k} = \mathrm{hp}_{\mathfrak{g},k+1,k} = \mathrm{hp}_{\mathfrak{g},k,k+1}$ *for* $k \geq 2$.

HP FOR FILIFORM LIE ALGEBRAS ASSOCIATED WITH $(5,7,10)$

Let $\mathfrak{g}$ be a filiform Lie algebra associated with the triple $(5,7,10)$ (that is, $\dim \mathfrak{g} = 10$, $z_1(\mathfrak{g}) = 5$ and $z_2(\mathfrak{g}) = 7$). Then we have $z_1^*(\mathfrak{g}) = 6$, and $z_2^*(\mathfrak{g}) = 4$. According to [1, Th. 1], there exists an adapted basis of $\mathfrak{g}$, $\{e_1, \ldots, e_{10}\}$, such that the law of $\mathfrak{g}$ is given by

$$\begin{aligned}
[e_1, e_h] &= e_{h-1} \quad \text{for } 3 \leq h \leq 10,\\
[e_{5+i}, e_8] &= \alpha_1 e_{i+2} + \alpha_2 e_{i+1} + \cdots + \alpha_{i+1} e_2 \quad \text{for } 0 \leq i \leq 2,\\
[e_5, e_{7+j}] &= \alpha_1 e_{j+1} + \gamma_1\, e_j + \cdots + \gamma_{j-1}\, e_2 \quad \text{for } 2 \leq j \leq 3,\\
[e_{5+k}, e_{7+\ell}] &= \sum_{h=2}^{k+\ell} P_h\left([e_{5+k-1}, e_{7+\ell}] + [e_{5+k}, e_{7+\ell-1}]\right) e_{h+1} + \beta_{k\ell}\, e_2,\\
&\qquad \text{for } 2 \leq \ell \leq 3,\ 1 \leq k \leq 1+\ell,
\end{aligned}$$

for a certain vector of complex numbers $(\underline{\alpha}, \underline{\gamma}, \underline{\beta}) \in \mathbb{C}^3 \times \mathbb{C}^2 \times \mathbb{C}^7 = \mathbb{C}^{12}$. After imposing the Jacobi identities $J(e_q, e_r, e_u)$, for $5 \leq q < r < u \leq 10$, we obtain the following three families of restrictions:

$$\begin{aligned}
U_1 &\equiv \{\alpha_1 = \alpha_2 = \gamma_1 = 0, \gamma_2 \neq 0, \alpha_3 \neq 0\},\\
U_2 &\equiv \{\alpha_1 = \gamma_1 = 0, \alpha_3 = -\frac{3}{7}\gamma_2 + \frac{2}{7}\beta_{1,2},\ \gamma_2 \neq 0,\ (\alpha_2, \alpha_3) \neq (0,0)\},\\
U_3 &\equiv \{\alpha_1 = 0, \alpha_3 = -\frac{3\gamma_2}{5} - \beta_{1,2}, \gamma_1 = -\alpha_2,\ (\alpha_2, \gamma_2) \neq (0,0),\ (\alpha_2, \alpha_3) \neq (0,0)\}.
\end{aligned}$$

Notice that each U_i is a Zariski locally closed subset in $\mathbb{C}^{12}$. Write $U_i = Z_i \cap G_i$ where Z_i, (resp. G_i) is the obvious Zariski closed set (resp. the obvious open set) in $\mathbb{C}^{12}$. We can also write $U_i = Z_i \cap G$ where G is the Zariski open set in $\mathbb{C}^{12}$ defined by the following two inequalities: $(\alpha_2, \alpha_3) \neq (0,0)$, and $(\gamma_1, \gamma_2) \neq (0,0)$. In particular, $U := U_1 \cup U_2 \cup U_3 = (Z_1 \cup Z_2 \cup Z_3) \cap G$ is also a locally closed set. Each point in U is identified with its associated filiform Lie algebra. If $\Gamma \subset \{1,2,3\}$ is not the empty set, we define

$$U_\Gamma = \left(\bigcap_{i \in \Gamma} U_i\right) \setminus \left(\bigcup_{j \in \Gamma^c} U_j\right)$$

where Γ^c is the complement of Γ in $\{1,2,3\}$.

Notice that $U_\Gamma = \varnothing$ if Γ has two elements. We now compute $\mathrm{HP}_{\mathfrak{g}}^{(2)}(t,s)$ for $\mathfrak{g} \in U_\Gamma$ for each Γ. Recall that for $\mathfrak{g} \in U$ we have $z_2^*(\mathfrak{g}) = 4$. Then, by Lemma 2, one has $[C^4\mathfrak{g}, C^4\mathfrak{g}] = \{0\}$. We also have the following equalities

$$[C^3\mathfrak{g}, C^6\mathfrak{g}] = \{0\},\ [C^3\mathfrak{g}, C^5\mathfrak{g}] = \langle \alpha_2 e_2 \rangle,\ [C^3\mathfrak{g}, C^4\mathfrak{g}] = [C^3\mathfrak{g}, C^3\mathfrak{g}] = \langle \alpha_2 e_2, \alpha_2 e_3 + \alpha_3 e_2 \rangle.$$

Moreover, we have

$$[C^2\mathfrak{g}, C^7\mathfrak{g}] = \{0\},\ [C^2\mathfrak{g}, C^6\mathfrak{g}] = \langle \gamma_1 e_2\rangle,\ [C^2\mathfrak{g}, C^5\mathfrak{g}] = \langle \gamma_1 e_2,\ \alpha_2 e_2,\ (\alpha_2+\gamma_1)e_3 + \beta_{12}e_2\rangle,$$
$$[C^2\mathfrak{g}, C^4\mathfrak{g}] = [C^2\mathfrak{g}, C^5\mathfrak{g}] + \langle \alpha_2 e_3 + \alpha_3 e_2,\ (2\alpha_2+\gamma_1)e_4 + (\alpha_3+\beta_{12})e_3 + \beta_{22}e_2\rangle,$$
$$[C^2\mathfrak{g}, C^3\mathfrak{g}] = [C^2\mathfrak{g}, C^2\mathfrak{g}] = [C^2\mathfrak{g}, C^4\mathfrak{g}] + \langle (2\alpha_2+\gamma_1)e_5 + (\alpha_3+\beta_{12})e_4 + \beta_{22}e_3 + \beta_{32}e_2\rangle.$$

In order to simplify the notation, we encode the coefficients $\mathrm{hp}_{\mathfrak{g},k,\ell}$ of the polynomial $\mathrm{HP}^{(2)}_{\mathfrak{g}}$ into two vectors:

$$\mathrm{hp}_{\mathfrak{g},3} := (\mathrm{hp}_{\mathfrak{g},3,5}, \mathrm{hp}_{\mathfrak{g},3,4}) \quad \text{and} \quad \mathrm{hp}_{\mathfrak{g},2} := (\mathrm{hp}_{\mathfrak{g},2,6}, \mathrm{hp}_{\mathfrak{g},2,5}, \mathrm{hp}_{\mathfrak{g},2,4}, \mathrm{hp}_{\mathfrak{g},2,3}),$$

having in mind that, by Lemma 2, one has $\mathrm{hp}_{\mathfrak{g},3,4} = \mathrm{hp}_{\mathfrak{g},3,3}$ and $\mathrm{hp}_{\mathfrak{g},2,3} = \mathrm{hp}_{\mathfrak{g},2,2}$.

For $\mathfrak{g} \in U_{\{1,2,3\}}$ we have $\mathrm{hp}_{\mathfrak{g},3} = (0,1)$ and $\mathrm{hp}_{\mathfrak{g},2} = (0,1,2,3)$.

For $\mathfrak{g} \in U_{\{1\}}$ we have $\mathrm{hp}_{\mathfrak{g},3} = (0,1)$ and the value of $\mathrm{hp}_{\mathfrak{g},2}$ is given by the following table:

$$\begin{aligned}
&(0,0,2,3) && \text{if } \beta_{12} = 0;\\
&(0,1,1,1) && \text{if } \beta_{12} \neq 0, \alpha_3+\beta_{12} = 0, \beta_{2,2} = 0;\\
&(0,1,1,2) && \text{if } \beta_{12} \neq 0, \alpha_3+\beta_{12} = 0, \beta_{2,2} \neq 0;\\
&(0,1,2,3) && \text{if } \beta_{12} \neq 0, \alpha_3+\beta_{12} \neq 0.
\end{aligned}$$

For $\mathfrak{g} \in U_{\{2\}}$ we have $\mathrm{hp}_{\mathfrak{g},3} = (1,2)$ and $\mathrm{hp}_{\mathfrak{g},2} = (0,2,3,4)$. For $\mathfrak{g} \in U_{\{3\}}$ we have $\mathrm{hp}_{\mathfrak{g},3} = (1,2)$ and $\mathrm{hp}_{\mathfrak{g},2} = (1,1,3,4)$. So, the Hilbert polynomial distinguishes 6 isomorphism classes in the family of filiform Lie algebras associated with the triple $(5,7,10)$.

Acknowledgements. The first author has been partially supported by PID2020-117800GB-I00, PID2024-158365OB-C22 and FQM-326 and grant SOL2024-30793 (PPI 2024-25 Universidad de Sevilla). The second author has been partially supported by Proyecto PID2020-117843GB-I00, and Proyecto PID2024-156912N funded by MICIU/AEI/10.13039/501100011033, and FEDER, UE.

References

[1] F.J. Castro-Jiménez, M. Ceballos: Bracket ideals and Hilbert polynomial of filiform Lie algebras. *ArXiv:2505.01241* (2025).

[2] F.J. Echarte, J. Núñez, F. Ramírez: Study of two invariants in complex filiform Lie algebras. *Algebras Groups Geom.* **13**, 55–70 (1996).

[3] F.J. Echarte, J. Núñez, F. Ramírez: Relations among invariants of complex filiform Lie algebras. *Appl. Math. Comput.* **147**, 365–376 (2004).

[4] D.R. Grayson, M.E. Stillman: Macaulay2, a software system for research in algebraic geometry. `http://www2.macaulay2.com`

[5] N. Jacobson: *Lie algebras.* Dover (1979).

[6] Maplesoft: Maple. `https://www.maplesoft.com`

[7] M. Vergne: *Variété des algèbres de Lie nilpotentes*. Thèse 3e cycle, Paris (1966).

[8] M. Vergne: Cohomologie des algèbres de Lie nilpotentes. Application à l'étude de la variété des algèbres de Lie nilpotentes. *Bull. Soc. Math. France* **98**, 81–116 (1970).

Birational biquadratic planar maps

C. Checa*, P. Mazón◇†

◇ *Speaker at EACA 2026*

* *Department of Mathematical Sciences, University of Copenhagen*

† *Department of Mathematics, CUNEF Universidad*

ccn@math.ku.dk, pablo.mazon@cunef.edu

Abstract. We prove that a rational map $\phi : \mathbb{P}^1 \times \mathbb{P}^1 \dashrightarrow \mathbb{P}^2$ with biquadratic entries is birational if and only if its differential $d\phi : \mathscr{T}_{\mathbb{P}^1\times\mathbb{P}^1} \dashrightarrow \phi^*\mathscr{T}_{\mathbb{P}^2}$ can be written as the sum of two tangent fields on $\mathbb{P}^2$, where (1) each field defines the tangent foliation to a pencil of conics, and (2) the two pencils share three distinct simple base points. Additionally, we provide a formula for $d\phi$ expressed solely in terms of these conics and standard multilinear operations. To this goal, we prove that the exterior product of two ternary quadrics is a (globally defined) tangent field to all the conics in the pencil they define.

We apply our results to develop effective methods for constructing birational maps with sufficient flexibility for applications. Our approach relies on control points and their associated weights. For suitably constrained control points, we prove that birationality is achieved if and only if the weights determine a point in the Segre-Veronese embedding of $\mathbb{P}^1 \times \mathbb{P}^1$ of degree $(2, 2)$, which reduces to a rank-one condition on a partially symmetric tensor.

Introduction

Rational maps are a central object of study in algebraic geometry, from both theoretical and applied perspectives. Determining the existence of a rational inverse is of interest for maps between algebraic varieties defined by polynomials of various degrees. For projective and multiprojective domains, syzygy-based criteria [1, 4–6, 11, 12] and the theory of blow-up algebras [2, 14] have been established as very useful tools.

Let $\mathbb{P}^n$ be the complex projective n-space. In this paper we study rational maps

$$\phi : \mathbb{P}^1 \times \mathbb{P}^1 \dashrightarrow \mathbb{P}^2$$

$$(s_0 : s_1) \times (t_0 : t_1) \mapsto (f_0 : f_1 : f_2)$$

with $f_0, f_1, f_2 \in R = \mathbb{C}[s_0, s_1] \otimes \mathbb{C}[t_0, t_1]$ of bidegree $(2, 2)$, i.e. homogeneous and quadratic in each pair of variables, without a common factor. Our goal is two-fold:

1. Characterize the existence of a rational inverse, that is, birationality.
2. Develop effective methods for the construction of such birational maps.

J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, V. Sotomayor (eds.): Proceedings of the XIX EACA, pp. 108-112 (2026).
ISBN: 978-84-09-87277-0

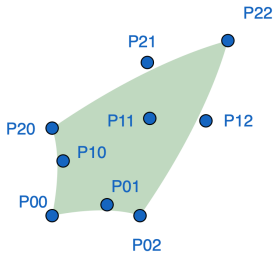


Figure 1. A biquadratic patch is defined by nine control points and their weights.

A useful formulation relies on control points and their associated weights (see Figure 1),

$$\Phi = (f_0, f_1, f_2) = \sum_{0 \le i,j \le 2} w_{ij} \mathbf{P}_{ij} b_i(s_0, s_1) b_j(t_0, t_1) \,,$$

where $\mathbf{P}_{ij} = (1, x_{ij}, y_{ij}) \in \mathbb{R}^3$ are the *control points* and $w_{ij} \in \mathbb{R}$ are their *weights*. Here, $b_0(s_0, s_1), b_1(s_0, s_1), b_2(s_0, s_1)$ is just a basis of $\mathbb{C}[s_0, s_1]_2$.

Previous Work

Regarding the problem of constructing birational maps $\psi : X \dashrightarrow \mathbb{P}^n$ with $\dim X = n$ and either $n = 2$ or $n = 3$, with sufficient flexibility for applications, current computational approaches remain restricted to low-degree parametrizations. For $n = 2$, an effective construction of maps $\psi : \mathbb{P}^1 \times \mathbb{P}^1 \dashrightarrow \mathbb{P}^2$ with bilinear entries appears in [13]. Concering biquadratic planar maps, the following result characterizes birationality in terms of syzygies.

Theorem 1. ([1, Lemma 13 and Theorem 16]) *Let $\phi : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^2$ be a dominant biquadratic map, and let $I = (f_0, f_1, f_2) \subset R$. The following are equivalent:*

1. *ϕ is birational*
2. *$\deg(I) = 6$ and the minimal free resolution of I is Hilbert-Burch*

$$0 \longrightarrow R(-3,-3)^2 \longrightarrow R(-2,-2)^3 \to I \longrightarrow 0.$$

For planar toric patches $\psi : T \dashrightarrow \mathbb{P}^2$, where T is a toric surface, birationality is also linked to rational linear precision [7, 8, 10]. Cremona transformations have also been used in the classification of Bézier patches via toric polar linear systems [9]. If $n = 3$, [3] provides methods for the generation and manipulation of birational maps $\phi : \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1 \dashrightarrow \mathbb{P}^3$ with trilinear entries. Here, birationality is characterized as rank-one condition on a tensor, and fixed-rank decomposition tools are exploited for the birational deformation of volumes.

Main Results

Let V be a $\mathbb{C}$-vector space of dimension n and $\boldsymbol{\lambda} = (\lambda_1 \ge \ldots \ge \lambda_\ell)$ an integer partition. If $V = \mathbb{C}^3$ we consider a basis e_0, e_1, e_2, and in the dual $V^\vee = (\mathbb{C}^3)^\vee$ we consider the dual basis x_0, x_1, x_2, i.e. $x_i(e_j) = \delta_{ij}$ for $0 \le i, j \le 2$. We denote by $\mathbf{S}_{\boldsymbol{\lambda}}(V)$ the image of V by

the Schur functor defined by $\boldsymbol{\lambda}$. If $V = (\mathbb{C}^{n+1})^\vee$, for $\boldsymbol{\mu} = (d)$ and $\boldsymbol{\nu} = (1, \dots, 1) = \mathbf{1}^d$ we obtain $\mathbf{S}_{\boldsymbol{\mu}} = S_d(V) \simeq \mathbb{C}[x_0, \dots, x_n]$ and $\mathbf{S}_{\boldsymbol{\eta}}(V) \simeq \bigwedge^d V$, that is, we recover the d-graded components of the symmetric and exterior algebras on V.

Lemma 2. *We have the isomorphisms of vector spaces*

$$\mathbb{P}\left(\bigwedge^2 (S_2(\mathbb{C}^3)^\vee)\right) \simeq \mathbb{P}\left(\mathbf{S}_{(3,1)}(\mathbb{C}^3)^\vee\right) \simeq \mathbb{P}\left(H^0(\mathbb{P}^2, \mathscr{T}_{\mathbb{P}^2}(1))\right) .$$

The previous lemma links $\bigwedge^2 (S_2(\mathbb{C}^3)^\vee)$ with (singular) foliations (of degree one) on $\mathbb{P}^2$, namely rank-one locally free subsheaves of the tangent sheaf $\mathscr{T}_{\mathbb{P}^2}$. The next result shows that the foliations of antisymmetric rank one, namely those that decompose as $c_0 \wedge c_1$ for some $c_0, c_1 \in S_2(\mathbb{C}^3)^\vee = \mathbb{C}[x_0, x_1, x_2]_2$, have as leaves all the plane conics in the pencil $\mathbb{C}\langle c_0, c_1\rangle = \{\lambda_0\, c_0 + \lambda_1\, c_1 : (\lambda_0 : \lambda_1) \in \mathbb{P}^1\}$.

Proposition 3. *Let $C_0, C_1 \subset \mathbb{P}^2$ be distinct smooth conics, $c_0, c_1 \in \mathbb{C}[x_0, x_1, x_2]$ their defining polynomials, and $P \in \mathbb{P}^2$. The following hold:*

1. *$\gamma = c_0 \wedge c_1 \in H^0(\mathbb{P}^2, \mathscr{T}_{\mathbb{P}^2}(1))$, i.e. γ defines a global vector field in $\mathbb{P}^2$ (of degree one)*
2. *If $P \in C_0 \cap C_1$ then $\gamma(P) = 0$*
3. *If $P \notin C_0 \cap C_1$ then $\gamma(P) \in \mathscr{T}_C|_P$ where C is the conic in $\mathbb{C}\langle c_0, c_1\rangle$ through P*

On the other hand, the differential of $\phi : \mathbb{P}^1 \times \mathbb{P}^1 \dashrightarrow \mathbb{P}^2$ induces a chain map

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathscr{O}_U^{\oplus 2} & \xrightarrow{(s_0\, s_1\, t_0\, t_1)} & \mathscr{O}_U(1,0)^{\oplus 2} \oplus \mathscr{O}_U(0,1)^{\oplus 2} & \longrightarrow & \mathscr{T}_U & \longrightarrow & 0 \\
 & & \| & & \downarrow{\scriptstyle D\phi} & & \downarrow{\scriptstyle d\phi} & & \\
0 & \longrightarrow & \mathscr{O}_U & \xrightarrow{(f_0\ f_1\ f_2)} & \mathscr{O}_{\mathbb{P}^2}(1)^{\oplus 3}\big|_{\phi(U)} & \longrightarrow & \mathscr{T}_{\mathbb{P}^2}\big|_{\phi(U)} & \longrightarrow & 0
\end{array}$$

where $U \subset \mathbb{P}^1 \times \mathbb{P}^1$ is a Zariski open set where $\phi|_U$ is a morphism. Here, the rows are restrictions of the Euler short exact sequences for $\mathbb{P}^1 \times \mathbb{P}^1$ and $\mathbb{P}^2$. The following is our main result.

Theorem 4. *Let $\phi : \mathbb{P}^1 \times \mathbb{P}^1 \dashrightarrow \mathbb{P}^2$ biquadratic. The following are equivalent:*

a) ϕ is birational, with inverse

$$\phi^{-1} : \mathbb{P}^2 \dashrightarrow \mathbb{P}^1 \times \mathbb{P}^1$$

$$(x_0 : x_1 : x_1) \mapsto (a_0 : a_1) \times (b_0 : b_1)$$

for some quadratic $a_i, b_j \in \mathbb{C}[x_0, x_1, x_2]$.

b) The base locus of ϕ is

$$P_1 \cup P_2 \cup P_3 \cup D$$

where the P_i are simple points and $D = (s, t)^2$ is a double point, for some linear $s \in \mathbb{C}[s_0, s_1]$, $t \in \mathbb{C}[t_0, t_1]$. Moreover, one of the P_i may be infinitely near to D. In

particular, the pencils of conics $\mathbb{C}\langle a_0, a_1\rangle$ and $\mathbb{C}\langle b_0, b_1\rangle$ have (1) one common conic, and (2) three common simple base points.

c) The differential $d\phi$ can be written as

$$d\phi \equiv (a_0 \wedge a_1)(\phi)\,\frac{(s_0 ds_1 - s_1 ds_0)}{s} + (b_0 \wedge b_1)(\phi)\,\frac{(t_0 dt_1 - t_1 dt_0)}{t}$$

for some linear $s \in \mathbb{C}[s_0, s_1]$ and $t \in \mathbb{C}[t_0, t_1]$.

Finally, we apply Theorem 4, $c)$ to obtain effective constructive results for birational bi-quadratic maps. We say that a configuration of control points is *birationally constrained* if there exist weights for which the associated map ϕ is birational.

Theorem 5. *For birationally constrained points, ϕ is birational if and only if the matrix*

$$M = \begin{pmatrix} \frac{w_{00}}{\Delta_{00}} & \frac{w_{01}}{\Delta_{01}} & \frac{w_{02}}{\Delta_{02}} \\ \frac{w_{10}}{\Delta_{10}} & \frac{w_{11}}{\Delta_{11}} & \frac{w_{12}}{\Delta_{12}} \\ \frac{w_{20}}{\Delta_{20}} & \frac{w_{21}}{\Delta_{21}} & \frac{w_{22}}{\Delta_{22}} \end{pmatrix}$$

for some $\Delta_{ij} \in \mathbb{C}$ (computed through the control points $\mathbf{P}_{ij}$), has partially symmetric rank one, namely we can write

$$M = \begin{pmatrix} \alpha_0^2\beta_0^2 & 2\alpha_0^2\beta_0\beta_1 & \alpha_0^2\beta_1^2 \\ 2\alpha_0\alpha_1\beta_0^2 & 4\alpha_0\alpha_1\beta_0\beta_1 & 2\alpha_0\alpha_1\beta_1^2 \\ \alpha_1^2\beta_0^2 & 2\alpha_1^2\beta_0\beta_1 & \alpha_1^2\beta_1^2 \end{pmatrix} \equiv (\alpha_0 s_0 + \alpha_1 s_1)^2\,(\beta_0 t_0 + \beta_1 t_1)^2$$

for some $(\alpha_0 : \alpha_1) \times (\beta_0 : \beta_2) \in \mathbb{P}^1_{\mathbb{C}} \times \mathbb{P}^1_{\mathbb{C}}$.

Example 6. Consider the configuration of nine control points in $\mathbb{A}^2_{\mathbb{R}}$ drawn in Figure 1, where

$$\begin{aligned} \mathbf{P}_{00} &= (1,2,2), & \mathbf{P}_{10} &= (1,\tfrac{21}{8},\tfrac{17}{8}), & \mathbf{P}_{20} &= (1,3,2), \\ \mathbf{P}_{01} &= (1,\tfrac{17}{8},\tfrac{21}{8}), & \mathbf{P}_{11} &= (1,\tfrac{28}{9},\tfrac{28}{9}), & \mathbf{P}_{21} &= (1,\tfrac{15}{4},\tfrac{37}{12}), \\ \mathbf{P}_{02} &= (1,2,3), & \mathbf{P}_{12} &= (1,\tfrac{37}{12},\tfrac{15}{4}), & \mathbf{P}_{22} &= (1,4,4)\,. \end{aligned}$$

These control points are birationally constrained, meaning that we can find weights that yield a birational map. For the choice of weights

$$w_{00} = 1\ ,\ w_{01} = -8\ ,\ w_{02} = 6\ ,\ w_{10} = 8\ ,\ w_{11} = -18\ ,\ w_{12} = 12\ ,$$

$$w_{20} = 6\ ,\ w_{21} = -12\ ,\ w_{32} = 7$$

the map ϕ given by the tuple $\Phi = (f_0, f_1, f_2) =$

$$\begin{pmatrix} s_0^2t_0^2 - 8s_0^2t_0t_1 + 6s_0^2t_1^2 + 8s_0s_1t_0^2 - 18s_0s_1t_0t_1 + 12s_0s_1t_1^2 + 6s_1^2t_0^2 - 12s_1^2t_0t_1 + 7s_1^2t_1^2 \\ 2s_0^2t_0^2 - 21s_0^2t_0t_1 + 18s_0^2t_1^2 + 17s_0s_1t_0^2 - 56s_0s_1t_0t_1 + 45s_0s_1t_1^2 + 12s_1^2t_0^2 - 37s_1^2t_0t_1 + 28s_1^2t_1^2 \\ 2s_0^2t_0^2 - 17s_0^2t_0t_1 + 12s_0^2t_1^2 + 21s_0s_1t_0^2 - 56s_0s_1t_0t_1 + 37s_0s_1t_1^2 + 18s_1^2t_0^2 - 45s_1^2t_0t_1 + 28s_1^2t_1^2 \end{pmatrix}$$

The map ϕ is not birational. Namely, a general point in $\mathbb{P}^2$ has 8 preimages by ϕ. However, an application of Theorem 4 tells us that updating the first weight $w_{00} = 1 \mapsto w_{00} = 3$ the new map is birational.

Acknowledgements. The first author was funded by the ERC under the grant agreement number 101044561. The second author was partially supported by the PRIN 2022 under the grant agreement 40104520.

References

[1] N. Botbol, L. Busé, M. Chardin, S.H. Hassanzadeh, A. Simis, Q.H. Tran: Effective criteria for bigraded birational maps. *J. Symbolic Comput.* **81**, 69–87 (2017).

[2] L. Busé, Y. Cid-Ruiz, C. D'Andrea: Degree and birationality of multi-graded rational maps. *Proc. Lond. Math. Soc.* **121**(4), 743–787 (2020).

[3] L. Busé, P. González-Mazón: Construction of birational trilinear volumes via tensor rank criteria. *SIAM J. Appl. Algebra Geom.* **9**(2), 405–431 (2025).

[4] L. Busé, P. González-Mazón, J. Schicho: Trilinear birational maps in dimension three. *Math. Comp.* **92**(342), 1837–1866 (2023).

[5] M. Chardin, S.H. Hassanzadeh, A. Simis: Degree of rational maps versus syzygies. *J. Algebra* **573**, 641–662 (2021).

[6] A.V. Doria, S.H. Hassanzadeh, A. Simis: A characteristic-free criterion of birationality. *Adv. Math.* **230**(1), 390–413 (2012).

[7] E. Duarte, B. Hollering, M. Wiesmann: *Toric fiber products in geometric modeling.* ISSAC 2023, 494–503. Springer (2023).

[8] L.D. Garcia Puente, F. Sottile: Linear precision for parametric patches. *Adv. Comput. Math.* **33**, 191–214 (2010).

[9] H.C. Graf von Bothmer, K. Ranestad, F. Sottile: Linear precision for toric surface patches. *Found. Comput. Math.* **10**(1), 37–66 (2009).

[10] R. Krasauskas: Toric surface patches. *Adv. Comput. Math.* **17**, 89–113 (2002).

[11] F. Russo, A. Simis: On birational maps and Jacobian matrices. *Compositio Math.* **126**, 335–358 (2001).

[12] F.O. Schreyer, K. Hulek, S. Katz: Cremona transformations and syzygies. *Math. Z.* **209**(3), 419–444 (1992).

[13] T.W. Sederberg, J. Zheng: Birational quadrilateral maps. *Comput. Aided Geom. Design* **32**, 1–4 (2015).

[14] A. Simis: Cremona transformations and some related algebras. *J. Algebra* **280**(1), 162–179 (2004).

Polynomial interpolation of a vector field on a convex polyhedral domain

J. Chu[◇*], S. Kaji[*]

[◇] *Speaker at EACA 2026*

[*] *Graduate School of Science, Kyoto University*

chujy626@gmail.com, kaji.shizuo.7r@kyoto-u.ac.jp

Abstract. We present a computational method for reconstructing a vector field on a convex polytope $\mathcal{P} \subset \mathbb{R}^d$ of arbitrary dimension from discrete samples. We specifically address the scenario where the vector field is subject to a no-penetration (slip) boundary condition, requiring it to be tangent to the boundary $\partial\mathcal{P}$. Given a degree bound k, our algorithm computes a polynomial vector field of degree at most k that fits the observed data in the least-squares sense while exactly satisfying the tangency constraints. Central to our approach is an explicit characterization of the module of polynomial vector fields tangent to $\partial\mathcal{P}$, derived using algebraic concepts from the theory of hyperplane arrangements.

Introduction

Reconstructing a vector field from sparse observations is a basic step in data-driven modeling of dynamics, ranging from particle tracking to reduced models in fluid mechanics. When the domain is bounded by rigid walls, physical consistency requires the *no–penetration* constraint: the velocity has vanishing normal component along the boundary. In practice, enforcing this constraint *exactly* is delicate: most regression procedures impose it only weakly, or require ad hoc penalty terms.

In this work we propose a computational scheme that enforces tangency to the boundary of a convex polytope $\mathcal{P} \subset \mathbb{R}^d$ by construction. For a prescribed degree bound k, we compute a polynomial vector field of degree $\leq k$ with minimal squared error to the observations, while satisfying the no-penetration boundary condition exactly. The key point is an algebraic characterization of tangent polynomial vector fields via logarithmic derivations of hyperplane arrangements, which allows us to build bases efficiently and robustly.

Problem formulation

Let $\mathcal{P} \subset \mathbb{R}^d$ be a convex polytope given by a minimal half-space representation

$$\mathcal{P} = \bigcap_{i=1}^{m} \{x \in \mathbb{R}^d \mid h_i(x) \leq 0\}, \qquad H_i = \{x \in \mathbb{R}^d \mid \langle \alpha_i, x \rangle + \ell_i = 0\} \tag{1}$$

J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, V. Sotomayor (eds.): Proceedings of the XIX EACA, pp. 113-117 (2026).
ISBN: 978-84-09-87277-0

where $\alpha_i \in \mathbb{R}^d \setminus \{0\}$ and $\langle\ ,\ \rangle$ denotes the standard inner product on $\mathbb{R}^d$. The hyperplane H_i is called a supporting hyperplane of $\mathcal{P}$. We are given observation pairs $\{(x_s, u_s)\}_{s\in\mathcal{O}}$ with $x_s \in \mathcal{P}$ and $u_s \in \mathbb{R}^d$.

For a degree bound $k \geq 0$ we denote by $\mathrm{Poly}(\mathcal{P})_{\leq k}$ the vector space of polynomial vector fields $\xi = (f_1, \ldots, f_d) : \mathcal{P} \to \mathbb{R}^d$ with $\deg f_q \leq k$. We encode the no-penetration boundary condition by requiring tangency along the boundary of $\mathcal{P}$, $\partial\mathcal{P}$:

$$\langle \alpha_i, \xi(x) \rangle = 0 \quad \text{for all } x \in \partial\mathcal{P}. \tag{2}$$

Since $\langle \alpha_i, \xi \rangle$ is a polynomial, (2) is equivalent to the *divisibility* condition

$$h_i \,\big|\, \langle \alpha_i, \xi \rangle \quad \text{in } \mathbb{R}[x_1, \ldots, x_d] \qquad (i = 1, \ldots, m). \tag{3}$$

This leads to the following space of admissible models.

Definition 1. Let $\mathrm{Poly}(\mathcal{P}) = \bigcup_{k\geq 0} \mathrm{Poly}_\partial(\mathcal{P})_{\leq k}$ denote the module of polynomial vector fields on $\mathcal{P}$. The module of *tangent polynomial vector fields* on $\mathcal{P}$ is

$$\mathrm{Poly}_\partial(\mathcal{P}) := \big\{ \xi \in \mathrm{Poly}(\mathcal{P}) \,\big|\, h_i \mid \langle \alpha_i, \xi \rangle \text{ for all } i \big\}.$$

For each $k \geq 0$, we set $\mathrm{Poly}_\partial(\mathcal{P})_{\leq k} := \mathrm{Poly}_\partial(\mathcal{P}) \cap \mathrm{Poly}(\mathcal{P})_{\leq k}$.

We formulate the reconstruction problem as the least-sqaures problem:

$$\xi^\star \in \operatorname{argmin} \xi \in \mathrm{Poly}_\partial(\mathcal{P})_{\leq k} \sum_{s\in\mathcal{O}} \|\xi(x_s) - u_s\|^2. \tag{4}$$

Tangent fields as logarithmic derivations

Let $S = \mathbb{R}[x_0, x_1, \ldots, x_d]$ and homogenize the affine forms h_i from (1) by

$$\hat{h}_i(x_0, x) = \langle \alpha_i, x \rangle + \ell_i x_0.$$

The hyperplanes $\hat{H}_0 := \{x_0 = 0\}$ and $\hat{H}_i := \{\hat{h}_i = 0\} \subset \mathbb{R}^{d+1}$ form a *central* arrangement $\hat{\mathcal{P}}$ with defining polynomial

$$Q_{\hat{\mathcal{P}}} := x_0 \prod_{i=1}^{m} \hat{h}_i \in S.$$

The logarithmic derivation module of $\hat{\mathcal{P}}$ is

$$D(\hat{\mathcal{P}}) := \Big\{ \theta \in \bigoplus_{p=0}^{d} S\frac{\partial}{\partial x_p} \mid \theta(\hat{h}_i) \in \hat{h}_i S \text{ for all } i \Big\}.$$

This is a graded S-module studied classically in the theory of hyperplane arrangements [2, 3]. Elements of $D(\hat{\mathcal{P}})$ may be interpreted as homogeneous polynomial vector fields tangent to all hyperplanes $\{\hat{H}_i \mid i = 0, 1, \ldots, d\}$.

Let $J(Q_{\hat{\mathcal{P}}})$ denote the Jacobian ideal generated by the partial derivatives $\frac{\partial Q_{\hat{\mathcal{P}}}}{\partial x_p}$ for $p = 0, \ldots, d$. The theory of logarithmic derivations yields an isomorphism

$$D(\hat{\mathcal{P}}) \cong \mathrm{syz}\big(J(Q_{\hat{\mathcal{P}}})\big) \oplus S(-1),$$

where $\mathrm{syz}\big(J(Q_{\hat{\mathcal{P}}})\big)$ denotes the syzygy module of $J(Q_{\hat{\mathcal{P}}})$. Building on this description, we obtain the following result, which is central to the efficiency of our algorithm.

Theorem 2. *There is an explicit isomorphism between* $\mathrm{Poly}_\partial(\mathcal{P})$ *and* $\mathrm{syz}\big(J(Q_{\hat{\mathcal{P}}})\big)$.

For computations we construct minimal homogeneous generators of $\mathrm{Syz}(J(Q_{\hat{\mathcal{P}}}))$ using Gröbner bases and Schreyer's algorithm [4].

Reconstruction algorithm

Once a basis $\{\phi^j\}_{j=1}^N$ of $\mathrm{Poly}_\partial(\mathcal{P})_{\leq k}$ is available through (2), our main problem (4) reduces to a linear least-squares problem. Our construction can be implemented[1] as an explicit algorithm as in Algorithm 1.

Algorithm 1: Find a polynomial vector field in $\mathrm{Poly}_\partial(\mathcal{P})_{\leq k}$ with minimal error

procedure FindPolyTangentialWithDegreeBound($k, \{(x_s, u_s) \mid s \in \mathcal{O}\}$)
  Require: $k \geq 0$, observation data $\{(x_s, u_s)\}_{s\in\mathcal{O}}$.
  Compute a set of minimal homogeneous generators for the $\mathbb{R}[x_0, x_1, \ldots, x_d]$-module $\mathrm{Syz}(J(Q_{\hat{\mathcal{P}}}))$.
  From these generators, construct an $\mathbb{R}$-basis $\{\hat{\phi}^j\}_{j=1}^N$ of degree up to k.
  Dehomogenize the basis by setting $x_0 = 1$: $\phi^j(x_1, \ldots, x_d) := \hat{\phi}^j(1, x_1, \ldots, x_d) \in \mathrm{Poly}_\partial(\mathcal{P})_{\leq k}$.
  Form the matrix A where $A_{s,j} = \phi^j(x_s)$.
  Form the vector b from u_s.
  Find coefficients $c = (c_j)_{j=1}^N$ that minimize $\|Ac - b\|^2$ (least-squares problem).
  Let the resulting vector field be $\xi(x) = \sum_{j=1}^N c_j\, \phi^j(x)$.
  return ξ;
end procedure

The construction guarantees *exact* tangency on each edge because the divisibility conditions (3) are enforced symbolically before any numerical fitting. In contrast, penalty-based methods typically approximate tangency only at a finite set of boundary points. This exactness is particularly useful when reconstructed fields are integrated numerically over long times, since spurious normal components can accumulate and lead to unphysical boundary crossing.

Example and discussion

We illustrate our method using a regular pentagon as the domain $\mathcal{P} \subset \mathbb{R}^d$ with $d = 2$. Let $\mathcal{P}$ be the convex hull of five points forming a regular pentagon. We solve the least-squares problem to find a best fitting tangential polynomial field of degree at most k; that is, to find an element in $\mathrm{Poly}_\partial(\mathcal{P})_{\leq k}$ which best interpolates the observations. The figures below show the results for $k = 4, 5$.

[1] An accompanying implementation is available in SageMath at `https://github.com/shizuo-kaji/HyperPlaneArrangementSAGE`.

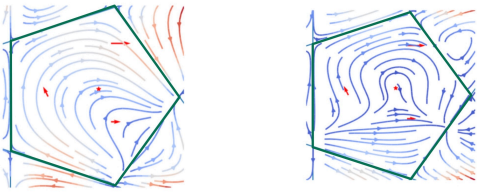


Figure 1. Reconstruction for the four observations indicated by red arrows, using degree 4 (left) and degree 5 (right). For degree 4, the fit exhibits a noticeable deviation from the observations, while with degree 5, the fitted vector field exactly interpolates the observations, resulting in zero error.

Our proposed method seamlessly accommodates constraints such as divergence-free and rotation-free (2). The former is of particular significance in fluid mechanics: a vector field in this space models an incompressible flow within a rigid container guaranteeing exact volume preservation.

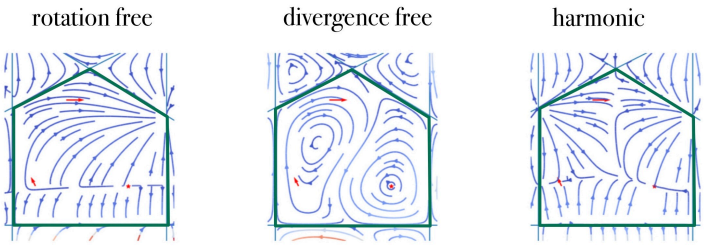


Figure 2. Tangency with additional constraints.

Future work includes studying degree bounds and minimal generators of $\mathrm{Poly}_\partial(\mathcal{P})$ to predict the smallest degree needed to reach a given accuracy threshold, motivated by recent results on logarithmic derivation modules [1].

Acknowledgements. This research was partially supported by JST Moonshot R&D Grant Number JPMJMS2021, and KAKENHI, Grant-in-Aid for Scientific Research (B) 25K00921 and (S) 25H00399.

References

[1] J. Chu: Free resolution of the logarithmic derivation modules of close to free arrangements. *J. Algebraic Combin.* **61**(2), Paper No. 26 (2025).

[2] P. Orlik, H. Terao: *Arrangements of hyperplanes*. Grundlehren der mathematischen Wissenschaften **300**, Springer (1992).

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

[4] F.O. Schreyer: A standard basis approach to syzygies of canonical curves. *J. Reine Angew. Math.* **421**, 83–123 (1991).

On the effective Pourchet's theorem

T. Cortadellas*, C. D'Andrea†, A.B. de Felipe‡ϟ, J. Hurtado‡, M.E. Montoro◇†

◇ *Speaker at EACA 2026*

* *Departament de Matemàtiques i Analítica de Dades, IQS School of Engineering, Universitat Ramon Llull*

† *Departament de Matemàtiques i Informàtica, Universitat de Barcelona*

‡ *Departament de Matemàtiques, Universitat Politècnica de Catalunya*

ϟ *Barcelona East School of Engineering (EEBE), and BarcelonaTech (UPC)*

teresa.cortadellas@iqs.url.edu, cdandrea@ub.edu, ana.belen.de.felipe@upc.edu, joel.hurtado@estudiantat.upc.edu, eula.montoro@ub.edu

Abstract. With the aid of Hensel Lemma, we refine the 2-adic Newton polygon algorithm proposed in [KMV23] to express computationally a given positive univariate polynomial with rational coefficients as a sum of five squares of rational polynomials –the effective Pourchet's Theorem– and extend it to cover almost all the possible inputs. We also provide examples which are covered with our methods but cannot be detected by previous conjectural algorithms.

Pourchet's Theorem [Pou71, Corollaire 4] states that any polynomial $f(x) \in \mathbb{Q}[x]$ such that $f(t) > 0$ for all $t \in \mathbb{R}$ can be expressed as

$$f(x) = f_1(x)^2 + f_2(x)^2 + f_3(x)^2 + f_4(x)^2 + f_5(x)^2, \tag{1}$$

with $f_i(x) \in \mathbb{Q}[x]$, $1 \leq i \leq 5$. This result, combined with the fact that there are polynomials with rational coefficients which cannot be sums of four squares (cf. [Pou71, Proposition 10]), shows that 5 is the minimal number of squares of rational polynomials needed to express *any* positive $f(x) \in \mathbb{Q}[x]$. Pourchet's Theorem can be reduced to the case $f(x) \in \mathbb{Q}[x]$ square-free, this is because if $f(x) = g^2(x)h(x)$ with $h(x)$ square-free and $h(t) > 0$, then $h(x) = \sum_{i=1}^{5} h_i^2(x)$ and therefore $f(x) = \sum_{i=1}^{5}(g(x)h_i(x))^2$.

Pourchet's original approach is based on local-global p-adic methods, in particular the Haase-Minkowski theorem, see [Raj93, Chapter 17] for a presentation of this result. Hence, in principle it is not suitable for an algorithmic adaptation. Recently, Magron, Koprowski and Vaccon had developed algorithms to express rational polynomials as sums of two squares ([KMV23, Algorithm 1]) and three or four squares ([KMV23, Algorithm 5]) if that decomposition was possible. They went further to propose that one can substract to a positive $f(x) \in \mathbb{Q}[x]$, a suitable even power (i.e. a rational square) of $\frac{1}{2}$ to produce a decomposition in a sum of 4 squares which could be treated algorithmically. This is the content of their Algorithm 6 in [KMV23]. Their approach is proven to work provided that the 2-adic valuation of either the constant or the leading coefficient of $f(x)$ is odd, and it is because of this obstruction that they are able to produce an algorithm ([KMV23, Algorithm 7]) which decomposes any posi-

J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, V. Sotomayor (eds.): Proceedings of the XIX EACA, pp. 118-121 (2026).
ISBN: 978-84-09-87277-0

tive rational $f(x)$ as a sum of 6 squares of rational polynomials, one more than Pourchet's sharp bound.

At the end of that paper, the authors propose a procedure ([KMV23, Algorithm 9]), which they conjecture succeeds in producing a decomposition of any positive rational polynomial as in (1).

Our first main result (see the proof in [CDDHM25]) is a negative response to this conjecture.

Theorem 1. *Algorithm 9 in [KMV23] does not stop after any finite number of steps for the following family of polynomials:*

$$f_{k,N}(x) := \frac{4}{N^2}x^{2(2k+1)} + \frac{1}{N^2}x^{2k+1} + \frac{4}{N^2},$$

with $k = 0, 1, \ldots,\ N \in \mathbb{N}$ *odd,* $N > 64$.

The key aspect of this family of counterexamples is given in part by the fact that having leading or constant coefficients of odd 2-adic valuation is a necessary condition for the algorithms in [KMV23] to work, as the following extended family of examples show.

Proposition 2. *Let* $a \in \mathbb{Z}_{>0}$. *If* $f(x) = g(x)^2 + 8a - 1$ *with* $g(x) \in \mathbb{Z}[x]$ *of degree* $d = 2k+1$ *and* $k \in \mathbb{Z}_{\geq 0}$, *then the procedure of Algorithm 6 in [KMV23] fails, i.e. the hypothesis on the* 2*-adic valuation of the leading coefficient of* $f(x)$ *is necessary.*

Even though Theorem 1 implies that [KMV23, Algorithm 9] does not solve the effective Pourchet problem in its full generality, still we can show that a modification of it actually works in more cases than those shown in that paper. For instance, if the degree of $f(x)$ is a multiple of 4, the following modification of Algorithm 5 in [KMV23] works independently of the valuation of the leading coefficient of $f(x)$.

Theorem 3. *Algorithm 1 stops after a finite number of steps and gives the right answer.*

The proof of this result can be found in [CDDHM25]. It still remains to find an algorithm to make explicit Pourchet's theorem for more cases than those covered so far. By using the Newton polygon method -as in that paper- we can cover more situations like the following.

Theorem 4. *Let* $f(x) \in \mathbb{Z}[x]$ *be a polynomial of (even) degree* d *such that* $f(t) > 0$ *for all* $t \in \mathbb{R}$, *and* $f(0) = 2^{2a}(4k+3)$ *with* $a, k \in \mathbb{Z}_{\geq 0}$. *Then, there exist* $N,\ell \in \mathbb{N}$, N *odd such that* $f(x) - \left(\frac{1}{2^\ell}x^{d/2} + \frac{2^a}{N}\right)^2$ *is a sum of four squares.*

The proof of this statement can be found in [CDDHM25]. Note that even though the family $f_{k,N}(x)$ of Theorem 1 does not fit directly with this claim, it turns out that the polynomial $N^2 \cdot f_{k,N}(x-1)$ satisfies the hypothesis of Theorem 4, and hence one cand find five elements in $\mathbb{Q}[x]$ such that the sum of their squares is equal to this polynomial. From here it is straightforward to get an expression of $f_{k,N}(x)$ as in (1).

One of the novelties of Theorem 4 is that we replace the constant $(\frac{1}{2^\ell})^2$ by the square of a polynomial of degree $d/2$. We will see in the proof of this result that we also use the 2-adic

Algorithm 1:

Input : A positive square-free polynomial $f(x) = c_0 + c_1 x + \ldots + c_d x^d \in \mathbb{Q}[x]$ of degree $d = 4d_0$, which is not a sum of 4 squares. The 2-adic valuations of the coefficients of $f(x)$ are $k_j := \mathrm{ord}_2(c_j)$ for $0 \leq j \leq d$.

Output : A polynomial $h(x) \in \mathbb{Q}[x]$ such that $f(x) - h(x)^2$ is a sum of 4 squares.

begin
  if k_d *is odd* **then**
    apply Algorithm 6 in [KMV23] to the input.
  else
    Find a positive number ε such that $\varepsilon < \inf\{f(x),\, x \in \mathbb{R}\}$.
    Set $l_1 := \lceil -\frac{1}{2} \cdot \log \varepsilon \rceil$.
    Set $l_2 := \lceil -\frac{k_0}{2} \rceil + 1$.
    Set $l_3 := \left\lceil \max\left\{ \frac{jk_d - dk_j}{2d - 2j},\ 0 < j < d \right\} \right\rceil$.
    Initialize $l := \max\{l_1, l_2, l_3\}$.
    while $\gcd(d, 2l + k_d) \neq 2$ **do**
      $l := l + 1$.
    end
    return $h(x) := 2^{-l}$.
  end
end

«Newton polygon test» which was the main tool in [KMV23] to prove that our proposed input is a sum of four squares of rational polynomials.

It turns out that one can also use the p-adic Hensel Lemma to get more flexibility and produce new decompositions of a positive $f(x) \in \mathbb{Q}[x]$ as a sum of five squares. The following theorems are proven by using this method.

Theorem 5. *Let $f(x) \in \mathbb{Z}[x]$ be a square-free polynomial of degree $d = 4k$, $k \in \mathbb{N}$. If $f(t) > 0$ for all $t \in \mathbb{R}$, then there exists $\ell_0 \in \mathbb{N}$ such that if $\ell \geq \ell_0$,*

$$f(x) - \frac{1}{2^{2\ell}}(x^2 + x + 1)^{2k}$$

is a sum of four squares in $\mathbb{Q}[x]$.

The proof of this claim can be found in [CDDHM25]. It is easy to verify that if a square-free $f(x)$ is such that $f(t) > 0$ for all $t \in \mathbb{R}$, then for all $g(x) \in \mathbb{R}[x]$ of degree bounded by d, there exists $\ell_0 \in \mathbb{N}$ such that if $\ell \geq \ell_0$, $f(t) - \frac{1}{2^{2\ell}} g(t) > 0$, and one can find this bound algorithmically.

Theorem 6. *Let $f(x) \in \mathbb{Z}[x]$ be a square-free polynomial of degree $d = 2(2k+1)$, $k \in \mathbb{N}$, such that $f(t) > 0$ for all $t \in \mathbb{R}$. Then, there exists $\ell_0 \in \mathbb{N}$ such that if $\ell \geq \ell_0$,*

$$f(x) - \frac{1}{2^{2\ell}}(x^2+x+1)^{2k}x^2$$

is a sum of four squares if $f(0)$ *is not of the form* $2^{2a}(8b+1)$*, with* $a, b \in \mathbb{Z}_{\geq 0}$*. If this is not the case, then this expression fails to be a sum of four squares for* $\ell \gg 0$ *and* $f(x)$*.*

The proof of this result can be found in [CDDHM25]. Integers of the form $2^{2a}(8b+1)$ are squares in $\mathbb{Z}_2$, the ring of 2-adic integers, and all squares in this ring are of this form. The condition on the constant coefficient of $f(x)$ in the hypothesis of Theorem 6 looks rather artificial, and one may argue that after a linear change of variables $f(x+\alpha)$, which does not change the structure of being a sum of four or five squares as we have done above with $f_{kN}(x)$ above, we just have to look for $\alpha \in \mathbb{Q}$ such that $f(\alpha)$ is not a square in $\mathbb{Q}_2$. If one finds such a change, then Theorem 6 would work in all the cases. But unfortunately, this cannot always be done as the following example due to Przemyslaw Koprowski shows:

$$4x^6 + 4x^3 + 9 = (1+2x^3)^2 + 8$$

is a polynomial such that evaluated in any rational number gives a square in $\mathbb{Q}_2$ and it is not the square of any polynomial. So, we cannot claim that with Theorems 5 and 6 we cover all the positive rational polynomials, and extra work is needed in order to have a complete effective approach to Pourchet's Theorem.

Acknowledgements. The first author has been partially supported by the Spanish MICINN research project PID2022-137283NB-C22. The second author has been partially supported by the Spanish State Research Agency, through the Severo Ochoa and María de Maeztu Program for Centers and Units of Excellence in R&D (CEX2020-001084-M), and the European H2020-MSCA-ITN-2019 research project GRAPES and the Spanish MICINN research project PID2023-147642NB-I00. The third author has been partially supported by the AGAUR project 2021 SGR 00603. The fifth author was partially supported by the Spanish MICINN research project PID2021-124827NB-I00, and by «ERDF A way of making Europe» by the European Union.

References

[CDDHM25] T. Cortadellas Benítez, C. D'Andrea, A.B. de Felipe, J. Hurtado Moreno, M.E. Montoro: *On the effective Pourchet's Theorem. ArXiv:2511.11783* (2025).

[KMV23] P. Koprowski, V. Magron, T. Vaccon: *Pourchet's theorem in action: decomposing univariate nonnegative polynomials as sums of five squares.* Proceedings of ISSAC 2023, 425–433. ACM (2023).

[Pou71] Y. Pourchet: Sur la représentation en somme de carrés des polynômes à une indéterminée sur un corps de nombres algébriques. *Acta Arith.* **19**, 89–104 (1971).

[Raj93] A.R. Rajwade: *Squares.* London Mathematical Society Lecture Note Series **171**, Cambridge University Press (1993).

Toric Euler-Jacobi vanishing theorem and zeros at infinity

C. D'Andrea[◇*], A. Dickenstein[†]

[◇] *Speaker at EACA 2026*

[*] *Departament de Matemàtiques i Informàtica, Universitat de Barcelona, and Centre de Recerca Matemàtica*

[†] *Departamento de Matemática, FCEN, Universidad de Buenos Aires*

cdandrea@ub.edu, alidick@dm.uba.ar

Abstract. We compute eigenfunctions for commuting ordinary differential operators (ODOs). Given an operator L with non-trivial centralizer, we design a symbolic algorithm to compute the eigenfunction of all operators in the centralizer (called the Baker-Akhiezer function). In this presentation we restrict to the algebro-geometric case, where the existence of operators of coprime order is guaranteed. Our algorithm is implemented in the `dalgebra` package of SageMath.

Jacobi started his 1835 paper in latin *New algebraic theorems on systems of two equations in two unknowns* [Jac35] with the following mention to **Euler's theorem**: «Of the theorems expressed in algebraic terms, there is hardly any more useful where equations are involved than the following, well-known one: If X is a polynomial in x, we have that

$$\sum \left(\frac{U}{\frac{dX}{dx}} \right) = 0,$$

if the sum runs over all roots x of the equation $X = 0$, and U is a polynomial in x of degree two less than the degree of X.»

His aim was to prove that this theorem can be extended to a system of two algebraic equations with two unknowns. We state his main result, translated into English.

Theorem. (Jacobi) *Let f, φ be polynomials in two variables x, y; let F be any other polynomial of degree smaller than the sum of the degrees of f and φ minus 2; it will be*

$$\sum \frac{F}{f'(x)\varphi'(y) - f'(y)\varphi'(x)} = 0, \tag{1}$$

the sum runs over all values x, y that are common roots of the equations $f = 0, \varphi = 0$.

Note that the denominator is a way of writing the *Jacobian* $J_{f,\varphi}$ of f and φ, that Jacobi introduced later in 1841! He didn't write two hypotheses. The first one is that the jacobian *does not vanish* at the common roots, and this was also an omitted hypothesis in the statement of Euler's theorem, where it is assumed that all roots of the input polynomial are simple (that is, the derivative does not vanish at any of the roots).

J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, V. Sotomayor (eds.): Proceedings of the XIX EACA, pp. 122-126 (2026).
ISBN: 978-84-09-87277-0

Khovanskii suggested to us the following nice proof of Euler's theorem. Let f be a univariate polynomial with complex coefficients of degree d, with distinct roots $\xi_1, \ldots, \xi_d$. Thus, $f = a_d \prod_{i=1}^{d}(x - \xi_i)$, with $a_d \neq 0$. Let $L_i(x) = \frac{\prod_{j\neq i}(x-\xi_j)}{\prod_{j\neq i}(\xi_i-\xi_j)}$ be the associated Lagrange interpolating polynomial (of degree $d-1$). For any polynomial h with $\deg(h) \leq d-1$, $h(x) = \sum_{i=1}^{d} h(\xi_i)\, L_i(x)$. So, the coefficient of x^{d-1} in this sum should be 0 if $\deg(h)$ is at most $d-2$. But this coefficient is precisely

$$0 = \sum_{i=1}^{d} h(\xi_i) \frac{1}{\prod_{j\neq i}(\xi_i - \xi_j)} = a_d \sum_{i=1}^{d} \frac{h(\xi_i)}{f'(\xi_i)}.$$

This result can be easily generalized to the case of possibly repeated roots by noting that $\frac{h(\xi_i)}{f'(\xi_i)}$ equals $2\pi i$ times the local *residue* of the differential form $\Phi_f(h) = \frac{h}{f}\, dx$ at ξ_i.

The second missing hypothesis in Jacobi's statement for the case of two variables is that f and φ have the Bézout number $\deg(f)\cdot\deg(\varphi)$ of isolated common roots in the complex plane, or equivalently, that f and φ do *not* have any common zeros at infinity in $\mathbb{P}^2$, as we will deduce from Theorem 3. Again, for each isolated common root (x_i, y_i) of f and φ the summand $\frac{F(x_i,y_i)}{J_{f,\varphi}(x_i,y_i)}$ equals $(2\pi i)^2$ times the local residue at (x_i, y_i) of the differential form $\frac{F}{f\cdot\varphi}\, dx \wedge dy$, see for instance [GH78]. Equality (1) asserts that the sum of local residues vanishes for any polynomial $F \in \mathbb{C}[x, y]$ with $\deg(F) < \deg(f) + \deg(\varphi) - 2$. Indeed, Euler and Jacobi theorems give vanishing conditions for the sum of residues in the projective compactifications of $\mathbb{C}$ and $\mathbb{C}^2$. Chapter 5 in [GH78] shows how classical geometric theorems in the projective plane are a consequence of this global vanishing.

There is a natural generalization of Jacobi's vanishing theorem to the multivariate case: given n polynomials $f_1, \ldots, f_n \in \mathbb{C}[x_1, \ldots, x_n]$ with isolated zeros $\xi_1, \ldots, \xi_m$ in $\mathbb{C}^n$ such that the sum of the corresponding intersection multiplicities equals the product of their degrees, the sum of local residues of the form $\frac{h}{f_1\cdots f_n}\, dx_1 \wedge \cdots \wedge dx_n$ over $\xi_1, \ldots, \xi_m$, is equal to zero if $\deg(h) < \deg(f_1) + \ldots + \deg(f_n) - n$. See for instance Corollary 4 in [AGV85, Chapter 5] or Theorem 7.10 in [Kun08].

And there is yet another generalization to the *sparse* setting. In this case, the role of $\mathbb{P}^n$ is played by a toric variety X_P which will be described below. The polynomials $f_1, \ldots, f_n$ can be *(multi)homogenized* to $F_1, \ldots, F_n$ in the *homogeneous coordinate ring* S of X_P [Cox95], so that it has sense to consider their zeroes in X_P.

The input data in the sparse context are n *lattice polytopes* $P_1, \ldots, P_n \subset \mathbb{R}^n$. We will always assume that their Minkowski sum $P = P_1 + \cdots + P_n$ is an n-dimensional lattice polytope and we will denote by P° its interior. We then consider Laurent polynomials $f_1, \ldots, f_n \in \mathbb{C}[\boldsymbol{t}^{\pm 1}] := \mathbb{C}[t_1^{\pm 1}, \ldots, t_n^{\pm 1}]$ with monomials $\boldsymbol{t}^{\boldsymbol{a}} = t_1^{a_1} \ldots t_n^{a_n}$ in $P_1, \ldots, P_n$:

$$f_i = \sum_{\boldsymbol{a}\in P_i\cap\mathbb{Z}^n} c_{i\boldsymbol{a}}\boldsymbol{t}^{\boldsymbol{a}},\ i = 1, \ldots, n, \tag{2}$$

and denote by $V_T(\boldsymbol{f}) = V_{(\mathbb{C}^*)^n}(f_1, \ldots, f_n)$ the variety of their common zeros in the n-torus $T = (\mathbb{C}^*)^n$, with $\mathbb{C}^* := \mathbb{C}\setminus\{0\}$. Bézout theorem is extended to the Bernstein-Kouchnirenko-Khvovanskii bound. Bernstein Theorem ([Ber75]) states that the degree $\deg(V_T(\boldsymbol{f}))$ of the zero dimensional part of $V_T(\boldsymbol{f})$ (the sum of the multiplicities of all its isolated zeroes over T)

is bounded by the mixed volume $\mathrm{MV}(P_1,\dots,P_n)$, and it is equal to this number when the polynomials have generic coefficients. There is a natural compactification of the n-torus T given by the compact toric variety X_P associated with the normal fan of P. Then, $X_P \setminus T = \cup_i D_i$, with one divisor D_i at infinity associated with any facet of P.

Given a sequence of n Laurent polynomials in n variables $f_1,\dots,f_n \in \mathbb{C}[\boldsymbol{t}^{\pm 1}]$ such that the variety $V_T(\boldsymbol{f})$ is finite, and any $h \in \mathbb{C}[\boldsymbol{t}^{\pm 1}]$, the *global residue* $\mathrm{Res}^T_{\boldsymbol{f}}(h)$ in T of the differential form $\omega_h := \frac{h}{f_1\dots f_n}\frac{dt_1}{t_1}\wedge\dots\wedge\frac{dt_n}{t_n}$, is defined as the sum of the local Grothendieck residues of ω_h at each of the points of $V_T(\boldsymbol{f})$:

$$\mathrm{Res}^T_{\boldsymbol{f}}(h) := \sum_{\boldsymbol{\xi}\in V_T(\boldsymbol{f})} \mathrm{Res}_{\boldsymbol{\xi}}(\omega_h). \tag{3}$$

A more informal characterization of this operator is the following: the *jacobian in the torus* is defined as $J^T_{\boldsymbol{f}} := \det\left(t_i\frac{\partial f_j}{\partial t_i}\right)_{1\le i,j\le n}$.

For $\boldsymbol{\xi} \in V_T(\boldsymbol{f})$, $\mathrm{Res}_{\boldsymbol{\xi}}(\omega_h)$ is equal to the value of $\frac{h(\boldsymbol{\xi})}{J^T_{\boldsymbol{f}}(\boldsymbol{\xi})}$ if $\boldsymbol{\xi}$ is a simple root of V, or to $\lim_{\varepsilon\to 0^+}\sum_{\boldsymbol{\xi}_\varepsilon}\frac{q(\boldsymbol{\xi}_\varepsilon)}{J^T_{\boldsymbol{f}_\varepsilon}(\boldsymbol{\xi}_\varepsilon)}$ of a deformed system $f_{\varepsilon,i}\to f_i$, $i=1,\dots,n$, the sum being over all $\boldsymbol{\xi}_\varepsilon \in V_T(\boldsymbol{f}_\varepsilon)$ which converge to $\boldsymbol{\xi}$ when $\varepsilon\to 0$. This limit always exists, see for instance [AGV85, S 5.11].

Global residues have important connections and applications in algebraic geometry, polynomial system solving and elimination theory. We have the following generalization of the Euler-Jacobi theorem to the toric setting from [Kho78, Theorem 2] under genericity hypotheses, then generalized in [CD97, Corollary 5]:

Theorem 1. (Toric Euler-Jacobi theorem) *Assume $V_T(\boldsymbol{f})$ is finite. If the sum of the local multiplicities at all the points $\xi \in V_{\boldsymbol{f}}$ equals $MV(P_1,\dots,P_n)$ (equivalently, the closures of the hypersurfaces $(f_i=0)$ do not have any common point of intersection at the divisors at infinity of X_P), then for any Laurent polynomial $h\in\mathbb{C}[\boldsymbol{t}^{\pm 1}]$ with monomials in the interior P° of P, the sum of local residues in* (3) *is equal to 0: $\mathrm{Res}^T_{\boldsymbol{f}}(h) = 0$.*

In our recent article ([DD26]), we explore the *necessity* of the hypothesis of not *having zeros* at the toric (and in particular, at the projective) infinity, that is: *is the (toric) Euler-Jacobi vanishing equivalent to this hypothesis*?

To address to this question, we need to introduce the following definition.

Definition 2. A sequence of polytopes $P_1,\dots,P_n$ is said to be *essential* if for any $k = 1,\dots,n$, and any $J\subset\{1,\dots,n\}$ of cardinality k, the dimension of $\sum_{j\in J}P_j$ is at least k. A sequence of polytopes $P_1,\dots,P_n$ is said to be *indecomposable* if it is essential and for any $k=1,\dots,n-1$, and any $J\subset\{1,\dots,n\}$ of cardinality k, either the dimension of $\sum_{j\in J}P_j$ is not equal to k, or if it this happens, there are no lattice points in the relative interior of this Minkowski sum with respect to the Euclidean topology.

We now state our first main result.

Theorem 3. ([DD26]) *Let $f_1, \dots, f_n \in \mathbb{C}[\boldsymbol{t}^{\pm 1}]$ be as in* (2) *with $P_1, \dots, P_n$ indecomposable. Assume that $V_T(\boldsymbol{f})$ is nonempty and that the intersection of the closures of the hypersurfaces $(f_i = 0)$ for $i = 1, \dots, n$, has dimension zero in the complete toric variety X_P associated with $P = P_1 + \cdots + P_n$. Then, the following are equivalent:*

i) $\deg(V_T(\boldsymbol{f})) = \mathsf{MV}(P_1, \dots, P_n)$.

ii) For any $h_0 \in \mathbb{C}[\boldsymbol{t}^{\pm 1}]$ with support contained in P°, $\mathrm{Res}^T_{\boldsymbol{f}}(h_0) = 0$.

iii) There is no Laurent polynomial $p_J \in \mathbb{C}[\boldsymbol{t}^{\pm 1}]$ with support contained in P° such that $J^T_{\boldsymbol{f}} \equiv p_J$ modulo the ideal $\langle f_1, \dots, f_n \rangle$ in $\mathbb{C}[\boldsymbol{t}^{\pm 1}]$.

In another but related direction, it is known that for a system of homogeneous polynomials $G_0, \dots, G_n \in \mathbb{C}[x_0, \dots, x_n]$, their standard jacobian belongs to the ideal $\langle G_0, \dots, G_n \rangle$ if and only if the variety they define in projective space $\mathbb{P}^n$ is empty [Spo89, Vas92]. In the sparse context, there is a notion of *toric jacobian* $J_{\boldsymbol{F}}$ and a more general *discrete jacobian* $\Delta_{\boldsymbol{F},\boldsymbol{\sigma}}$ for a system of (toric) homogeneous polynomials $F_0, \dots, F_n$ in the homogeneous coordinate ring S of X_P with ample degrees.

We now present our second main result:

Theorem 4. ([DD26]) *Let X be a complete toric variety and $F_i \in S_{\alpha_i}$ for $i = 0, \dots, n$, where each degree α_i is ample. Assume that $V_X(F_0, \dots, F_n) \neq \emptyset$ and that for some $i \in \{0, \dots, n\}$, the zero set $V_X(F_0, \dots, F_{i-1}, F_{i+1}, \dots, F_n)$ is finite. Then,*

1. *If $\boldsymbol{\sigma}$ is a flag of cones in Σ, then $\Delta_{\boldsymbol{F},\boldsymbol{\sigma}} \in \langle F_0, \dots, F_n \rangle$.*
2. *If in addition each of the α_i's is an integer multiple of a fixed ample Cartier degree α, then $J_{\boldsymbol{F}} \in \langle F_0, \dots, F_n \rangle$.*

Acknowledgements. The first author has been partially supported by the Spanish MICINN research projects PID2019-104047GB-I00 and PID2023-147642NB-I00. The second author has been partially supported by UBACYT 20020220200166BA and CONICET PIP 11220200100182CO, Argentina.

References

[AGV85] V.I. Arnold, S.M. Gusein-Zade, A.N. Varchenko: *Singularities of differentiable maps. Vol. I. The classification of critical points, caustics and wave fronts*. Monographs in Mathematics **82**, Birkhäuser Boston (1985).

[Ber75] D.N. Bernstein: The number of roots of a system of equations. *Funkcional. Anal. i Prilož.* **9**(3), 1–4 (1975).

[CD97] E. Cattani, A. Dickenstein: A global view of residues in the torus. *J. Pure Appl. Algebra* **117/118**, 119–144 (1997).

[Cox95] D. Cox: The homogeneous coordinate ring of a toric variety. *J. Algebraic Geom.* **4**(1), 17–50 (1995).

[DD26] C. D'Andrea, A. Dickenstein: Toric Euler-Jacobi vanishing theorem and zeros at infinity. *ArXiv:2601.13977* (2026).

[GH78] P. Griffiths, J. Harris: *Principles of algebraic geometry*. Pure and Applied Mathematics, Wiley-Interscience (1978).

[Jac35] C.G.J. Jacobi: Theoremata nova algebraica circa systema duarum aequationum, inter duas variabiles propositarum. *J. Reine Angew. Math.* **14**, 281–288 (1835).

[Kho78] A.G. Khovanskii: Newton polyhedra and the Euler-Jacobi formula. *Uspekhi Mat. Nauk* **33**(6), 237–238 (1978).

[Kun08] E. Kunz: *Residues and duality for projective algebraic varieties*. University Lecture Series **47**, American Mathematical Society (2008).

[Spo89] S. Spodzieja: On some property of the Jacobian of a homogeneous polynomial mapping. *Bull. Soc. Sci. Lett. Łódź* **39**(5), 6 pp. (1989).

[Vas92] W.V. Vasconcelos: The top of a system of equations. *Bol. Soc. Mat. Mexicana* **37**(1–2), 549–556 (1992).

Bounds for radii of compact semialgebraic sets defined over the rationals and archimedeanity

C. D'Andrea*, J. Hurtado Moreno◇†

◇ *Speaker at EACA 2026*

* *Departament de Matemàtiques i Informàtica, Universitat de Barcelona*

† *Departament de Matemàtiques, Universitat Politècnica de Catalunya*

cdandrea@ub.edu, joel.hurtado@estudiantat.upc.edu

Abstract. We present bounds for radii of balls containing all compact components of algebraic and semialgebraic sets defined over the rational numbers, improving previous results in the literature. These bounds are expressed in terms of the degrees and coefficients of the polynomials defining the set, the number of such polynomials, and the number of variables. As an application to non-negativity certificates for polynomials, we use these bounds to provide an effective approach to checking the archimedeanity of quadratic modules.

Introduction

Given a finite sequence of polynomials $g_1, \dots, g_s \in \mathbb{Z}[\bar{x}] = \mathbb{Z}[x_1, \dots, x_n]$, we are interested in estimating the radius of a ball centered at $\mathbf{0} \in \mathbb{R}^n$ containing all the compact compontents of the semialgebraic set

$$S(g) = \{\bar{x} \in \mathbb{R}^n \mid g_1(\bar{x}) \geq 0, \dots, g_s(\bar{x}) \geq 0\}.$$

As a first option, it is possible to approach this problem through a quantifier elimination algorithm. However, our aim is to obtain a bound for this radius depending only on the input data: degree and size of its coefficients.

These bounds provide an effective procedure for checking a key property related to non-negativity certificates for polynomials. This property is the archimedeanity of quadratic modules, and is crucial in this context as it is a standing assumption in many results such as [Put93, JP24, NS07, SCMK25].

Basu and Roy [BR10] found that it suffices to take the ball centered at the origin with radius

$$\sqrt{n}\left((2d+1)(2d)^{n-1}+1\right)2^{(2d)^{n-1}(2d+1)(n(2d-1)+2)(2h+n\log(d+1)+\log s+(n-1)\log 2d+2\log(2d+1)+3)}, \quad (1)$$

where $d = \max\{\deg(g_i), i = 1, \dots, s\}$, $h = \max\{h_{g_i}, i = 1, \dots, s\}$, and h_{g_i} denotes the *height* of g_i, that is, the logarithm of the maximum of the absolute values of its coefficients.

To prove this result, they study the problem of bounding a ball that contains the algebraic variety $V_{\mathbb{R}}(f) \subset \mathbb{R}^n$ for a given $f(\bar{x}) \in \mathbb{Z}[\bar{x}]$, and reduce the semialgebraic case to the

J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, V. Sotomayor (eds.): Proceedings of the XIX EACA, pp. 127-130 (2026).
ISBN: 978-84-09-87277-0

algebraic case. By improving the algebraic case, we automatically obtain improvements for the semialgebraic case.

What follows is a short version of our results improving (1), and its application to the study of archimedeanity of quadratic modules.

Bounds for algebraic hypersurfaces

Let $f(\bar{x}) \in \mathbb{Z}[\bar{x}]$ be a polynomial with degree d_f. Denote by $d_f^* = 2k \in \{d_f+1,\, d_f+2\}$ the smallest even number strictly larger than d_f, and let $g(\bar{x}) = \sum_{i=1}^n x_i^{2k}$.

The following is the classical Lagrange Multipliers Theorem adapted to our situation.

Theorem 1. *If $\bar{u} \in \mathbb{R}^n$ is a critical point of a C^1 function $h|_{V_{\mathbb{R}}(f)}$, there exists $\lambda \in \mathbb{R}$ such that $\nabla h(\bar{u}) = \lambda \nabla f(\bar{u})$.*

From this statement one deduces that all the local maximum and minima of $g(\bar{x})$ on $V_{\mathbb{R}}(f)$ are contained in the first components of solutions of the system of $n+1$ equations in $n+1$ unknowns $(x_1, \ldots, x_n, \lambda)$:

$$\left\{\begin{array}{rcl} f(\bar{x}) & = & 0 \\ 2kx_1^{2k-1} & = & \lambda \frac{\partial f}{\partial x_1} \\ \vdots & \vdots & \vdots \\ 2kx_n^{2k-1} & = & \lambda \frac{\partial f}{\partial x_n}. \end{array}\right. \tag{2}$$

In particular, if $C \subset V_{\mathbb{R}}(f)$ is a compact connected component, then $g(\bar{x})$ reaches its maximum in this set and any $\bar{u} \in C$ satisfying this maximum will be a solution of (2).

By proving that the system (2) is 0-dimensional in $\mathbb{C}[x_1, \ldots, x_n, \lambda]$, a bound on the height of its solutions can be obtained by applying directly results from [DKS13] on the height of solutions of polynomial systems defined over $\mathbb{Q}$. Next, by relating the 2-norm with the $2k$-norm in $\mathbb{R}^n$ defined by $g(\bar{x})^{\frac{1}{2k}}$, we obtain our first result.

Theorem 2. *Let $C \subset V_{\mathbb{R}}(f(\bar{x}))$ be a compact component. Then, any element in C has 2-norm bounded by*

$$\sqrt{n} e^{n(d_f+1)^{n-1}\left(2(h_f+d_f\ \log(n+1))+\log(d_f+2)+1\right)}.$$

This bound is sharper compared with the one obtained in [BR10, Theorem 1], which amounts to

$$\sqrt{n}\left((d_f+1){d_f}^{n-1}+1\right) 2^{{d_f}^{n-1}(d_f+1)(n(d_f-1)+2)(h_f+(n-1)\ \log d_f+2\ \log(d_f+1)+3)}.$$

Bounds for semialgebraic sets

Let us now consider a set of polynomials $g_1(\bar{x}), \ldots, g_s(\bar{x}) \in \mathbb{Z}[\bar{x}]$ such that $S(g) = \{\bar{x} \in \mathbb{R}^n \mid g_i(\bar{x}) \geq 0,\, i = 1, \ldots, s\} \subset \mathbb{R}^n$ has at least one compact connected component. Thanks to the proof of [BR10, Theorem 3], we know that in order to obtain a bound for the radius of any ball containing the compact connected components of $S(g)$, it suffices to apply

the bound obtained for the algebraic case to a polynomial f constructed as a sum of squares of a subfamily of the polynomials $g_1, \ldots, g_s$.

We just have to keep in mind that now this polynomial f has degree and height bounded by $2d$ and $2h+n\log(d+1)+\log s$ respectively, where d is an upper bound for all the degrees of $g_1, \ldots, g_s$, and h is an upper bound for the height of the coefficients of $g_1, \ldots, g_s$. With this we get

Theorem 3. *A bound for the radius of any ball centered at $0 \in \mathbb{R}^n$ containing any compact connected component of $S(g)$ is given by*

$$\sqrt{n}e^{n(2d+1)^{n-1}(2(2h+n\log(d+1)+\log s+2d\log(n+1))+\log(2d+2)+1)}.$$

Again, this is a slight improvement compared with (1), which was obtained in [BR10, Theorem 3].

Archimedeanity

In the context of certificates of non-negativity for polynomials, it is common to work with semialgebraic sets and quadratic modules. We define the quadratic module generated by $g_1, \ldots, g_s$ as

$$M(g) := \{\sigma_0 + \sigma_1 g_1 + \ldots + \sigma_s g_s | \sigma_0, \sigma_1, \ldots, \sigma_s \in \sum \mathbb{R}[x_1, \ldots, x_n]^2\},$$

where $\sum \mathbb{R}[x_1, \ldots, x_n]^2$ denotes the cone of sums of squares polynomials.

A key concept here is archimedeanity. We say that the quadratic module $M(g)$ is archimedean if there exists $N \in \mathbb{R}_{>0}$ such that

$$N - \sum_{i=1}^{n} x_i^2 \in M(g).$$

Putinar's Positivstellensatz [Put93] states that, if $M(g)$ is archimedean, then for every $f \in \mathbb{R}[x_1, \ldots, x_n]$, $f > 0$ in $S(g)$ implies that $f \in M(g)$.

This result transforms the problem of checking the positivity of a polynomial in a semialgebraic set into checking whether a polynomial belongs to the quadratic module generated by a set of polynomials, a problem that turns out to be computationally feasible. There are numerous subsequent works based on the property of archimedeanity, but there are no implementable algorithms to verify this property in the literature; only theoretical characterizations exist. Our last result is the following.

Assume that $S(g)$ is a compact set (otherwise $M(g)$ would not be archimedean, recalling that archimedeanity of $M(g)$ implies compactness of $S(g)$). Therefore, there exists $R > 0$ such that $S(g)$ is contained in the ball centered at $0 \in \mathbb{R}^n$ with radius R. Define

$$g_R(\bar{x}) := R^2 - (x_1^2 + \ldots + x_n^2).$$

Proposition 4. *$M(g)$ is archimedean if and only if $g_R \in M(g)$.*

This result gives an effective and sharp bound on the number R to test whether a certain quadratic module $M(g)$ is archimedean or not if $S(g)$ is a compact set. Additionally, it provides a computational approach, since, as mentioned above, checking whether a polynomial belongs to a quadratic module is a computationally feasible problem.

Now, in order to obtain a valid value for the radius, one may use a quantifier elimination algorithm or, more simply, as an application of the previous results, apply Theorem 3 to compute a suitable value of R.

Acknowledgements. The first author has been partially supported by the Spanish MICINN research projects PID2019-104047GB-I00 and PID2023-147642NB-I00.

References

[BR10] S. Basu, M.F. Roy: Bounding the radii of balls meeting every connected component of semi-algebraic sets. *J. Symbolic Comput.* **45**(12), 1270–1279 (2010).

[DKS13] C. D'Andrea, T. Krick, M. Sombra: Heights of varieties in multiprojective spaces and arithmetic Nullstellensatze. *Ann. Sci. Éc. Norm. Supér.* **46**(4), 549–627 (2013).

[JP24] G. Jeronimo, D. Perrucci: Rational certificates of non-negativity on semialgebraic subsets of cylinders. *J. Pure Appl. Algebra* **228**(6) (2024).

[NS07] J. Nie, M. Schweighofer: On the complexity of Putinar's Positivstellensatz. *J. Complexity* **23**, 135–150 (2007).

[Put93] M. Putinar: Positive polynomials on compact semi-algebraic sets. *Indiana Univ. Math. J.* **42**(3), 969–984 (1993).

[SCMK25] W. Shang, J.A. Castellanos Joo, C. Mou, D. Kapur: Computing Certificates of Strictly Positive Polynomials in Archimedean Quadratic Modules. *ArXiv:2503.11119* (2025).

On fibers and semi-algebraicity of ReLU neuromanifolds

A. Flinth*, S. Mereta◇†, M. Pernice‡

◇ *Speaker at EACA 2026*

* *Department of Mathematics and Mathematical Statistics, Umeå University*

† *Departamento de Matemáticas, CUNEF Universidad*

‡ *Department of Mathematics, University of Washington*

axel.flinth@umu.se, stefano.mereta@cunef.edu, mpernice@uw.edu

Abstract. We study the semi-algebraicity of the neuromanifold $\mathcal{M}_{\mathbf{N}}$ of a feedforward ReLU neural network and the fibers of its parametrization map. Studying the fibers in this setting reduces to characterizing all the ways in which a piecewise linear (PL) function f can be written as a difference of two convex piecewise linear (CPL) functions. We completely describe this fiber when we restrict the difference map to the finite dimensional space of PL functions whose skeleton is contained in a fixed one. In this case we also give a sufficient condition for minimality. Furthermore, we prove that $\mathcal{M}_{\mathbf{N}}$ is not a semi-algebraic quotient of the space of weights of the network. Finally, we introduce and study the notion of *honest* open subset of the space of weights, where the network does not show any *hidden symmetries* behavior. We conjecture that the maximal honest open is always semi-algebraic and prove that in the shallow case it is even Zariski.

A machine learning model can be viewed as a map

$$\mathcal{W} \times \mathcal{X} \to \mathcal{Y}$$

where $\mathcal{W}$ is a space of weights, $\mathcal{X}$ the space of inputs and $\mathcal{Y}$ the space of outputs. Given a pair $(w, x) \in \mathcal{W} \times \mathcal{X}$ we will denote its image as $f_w(x) \in \mathcal{Y}$. The space of functions $\mathcal{M} := \{f_w \colon \mathcal{X} \to \mathcal{Y} \mid w \in \mathcal{W}\}$ is called the *neuromanifold* associated to the model.

Training a model is an optimization process that aims to reach a point on the neuromanifold that is closest (with respect to a chosen loss function) to a given objective function. In practical settings, though, this optimization does not happen on the neuromanifold, but on the space of weights of the model. This can cause distortions, given for example by a singular parametrization of the neuromanifold: in this case, a critical weight for the parametrization map would be critical for the loss function, without being a genuine optimum for the loss function on the neuromanifold. Furthermore, critical points of the neuromanifold are more prone to be optima for the loss function, as their Voronoi cell can have higher dimension.

For the reasons above, in order to unveil the mysteries of the training process and make it more efficient, the theoretical study of the geometry of the neuromanifold has recently

J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, V. Sotomayor (eds.): Proceedings of the XIX EACA, pp. 131-135 (2026).
ISBN: 978-84-09-87277-0

experienced a quick development, under the name of *neuroalgebraic geometry* (see [7] for an overview).

The neuroalgebraic geometry of neural networks with polynomial activation functions is already fairly well understood (see for example [5, 6, 10, 13]). When dealing with polynomials there is a precise dictionary between machine learning terminology and algebro-geometric invariants attached to the neuromanifold, see [7, Table 1]. For non-polynomial activation function almost nothing is known about the geometry of the neuromanifold. In the present work we focus on the study of the neuromanifold of feedforward neural networks with *ReLU* (rectified linear unit) activation functions: $\mathrm{ReLU}(x) = \max(x, 0)$.

Notation

Let $L \in \mathbb{N}$ be the number of layers of a neural network and $N_k \in \mathbb{N}$ be the width of the k-th layer, for $k = 0, \dots, L$. With these choices, we say that the neural network considered is of architecture $\mathbf{N} := (N_0, \dots, N_L)$. Its number of weights is $M := \sum_{k=0}^{L} N_k(N_{k-1} + 1)$. In this setting, given $w \in \mathbb{R}^M$ the function f_w can be represented as a composition

$$f_w = W_L \circ \sigma \circ W_{L-1} \circ \cdots \circ \sigma \circ W_1$$

where W_k is an affine transformation $\mathbb{R}^{N_{k-1}} \to \mathbb{R}^{N_k}$ and the activation function σ is the ReLU. We will denote the neuromanifold of a ReLU network of architecture $\mathbf{n}$ as $\mathcal{M}_{\mathbf{n}}$. In our work we reduce to the case of zero bias (i.e. we assume the maps W_k to be linear) and $N_L = 1$: results obtained under these hypothesis can be extended back to the general setting.

Previous results

The study of the geometry of $\mathcal{M}_{\mathbf{N}}$ was already approached in [16] and [8]. Every function in $\mathcal{M}_{\mathbf{N}}$ is a continuous piecewise linear function $\mathbb{R}^{N_0} \to \mathbb{R}^{N_L}$ with finitely many linearity regions (PL function, for short). Conversely, in [17] it is proven that for any PL function $f\colon \mathbb{R}^{N_0} \to \mathbb{R}^N$ there exist a natural number L and an architecture $\mathbf{N} = (N_0, \dots, N_L = N)$ such that $f \in \mathcal{M}_{\mathbf{N}}$.

Every PL function is a pointwise difference of two continuous convex piecewise linear functions with finitely many linearity regions (CPL functions, for short). The choice of these CPL functions is highly non-unique. Since CPL functions are tropical signomial functions, we can look at PL functions as tropical rational (signomial) functions. This perspective allows us to study $\mathcal{M}_{\mathbf{n}}$ by using tools from tropical and polyhedral geometry.

The problem of identifiability for a ReLU neural network of architecture $\mathbf{N}$ is equivalent to understanding the fibers of the parametrization map

$$\Phi : \mathbb{R}^M \to \mathrm{PL} \qquad w \mapsto f_w.$$

This parametrization map can be regarded as a composition associating to a weight a pair of tropical signomials, to this a pair $(g, h) \in \mathrm{CPL}$ and lastly to such a pair the PL function $f = g - h$. As the first two maps are well understood, the problem reduces to characterize

the fibers of the difference map CPL $\times$ CPL $\to$ PL. As far as we know there are several partial results in this direction (e.g. [12, 14]), but no general characterization. In particular finding *minimal* elements in the fibers, i.e. CPL pairs such that the associated polytope pair are minimal with respect to polytope inclusion, has garnered significant interest. See for example [4, 9, 15].

Contribution 1: Functions in PL with a fixed skeleton

In our work, we firstly focus on the study of the fibers of the difference map restricted to the finite dimensional space PL_ϕ of piecewise linear functions whose skeleton (i.e. non-differentiability locus) is a subset of the skeleton of a fixed polyhedral fan ϕ with ℓ full-dimensional cells. From the combinatorial structure of ϕ, we build a matrix B_ϕ, called a *linear description* of ϕ. We then show that PL_ϕ essentially can be identified with the kernel of B_ϕ.

Theorem 1. *Let $\mathcal{L} \subset \mathsf{PL}_\phi$ be the subset of linear functions, then*

$$\mathsf{PL}_\phi / \mathcal{L} \cong \ker B_\phi \subseteq \mathbb{R}^{\ell(\ell-1)}$$

and the fiber $D_\phi^{-1}(f)$ of $f \in \mathsf{PL}_\phi$ is the intersection of a linear subspace with a translation of the positive quadrant in $\mathbb{R}^{\ell(\ell-1)}$.

A basis A of $\ker B_\phi$ is *non-negative* if $A \subset \mathbb{R}^{\ell(\ell-1)}_{\geq 0}$. We partially address the problem of minimality of decompositions over PL_ϕ.

Proposition 2. *Let $f \in \mathsf{PL}_\phi$ and set $b := \dim(\ker B_\phi)$. If there exists a non-negative basis for $\ker B_\phi$ then $D_\phi^{-1}(f) \neq \emptyset$. Furthermore if there exist two non-negative basis A, B of $\ker B_\phi$ such that $B^\top A = \mathrm{id}_{\mathbb{R}^b}$ then $D_\phi^{-1}(f) = (g_0, h_0) + \mathsf{CPL}_\phi$ for a unique pair (g_0, h_0).*

Contribution 2: The (non)semi-algebraic quotient structure of $\mathcal{M}_{\mathbf{n}}$

The neuromanifold of neural networks with polynomial activation functions is a semialgebraic subset of the space of polynomial of a certain degree dependent on the architecture. In the second part of our work we approach the semi-algebraicity of $\mathcal{M}_{\mathbf{n}}$ for ReLU networks. Let us denote as E_Φ the equivalence relation induced on the space of weights $\mathcal{W} = \mathbb{R}^M$ by the parametrization map Φ (i.e. $w \sim w'$ if $\Phi(w) = \Phi(w')$). The main theorem of [11] states an equivalence between the existence of the geometric quotient $\mathbb{R}^M / E_\Phi$ as a semi-algebraic space and the existence of a semi-algebraic subset K of $\mathcal{W}$ with a certain property. We provide an explicit counterexample to the existence of the set K, thus proving that

Theorem 3. *The neuromanifold $\mathcal{M}_{\mathbf{n}}$ of a ReLU neural network is in general not semi-algebraic as a quotient.*

Contribution 3: Hidden symmetries and honest parameter subsets

Finally, in order to have a better grasp on the fibers of the parametrization map in general, we introduce the space $\mathcal{P}$ obtained from the space of weights $\mathcal{W}$ by taking into account the action scaling and permutation i.e. the *trivial* symmetries of the network. In $\mathcal{P}$, we study what

we call *honest* open subsets, i.e. open subsets over which the fibers of the parametrization are trivial. We state the following

Conjecture 4. *Given a ReLU neural network of any architecture* $\mathbf{n}$*, the maximal honest open is a semi-algebraic subset of* $\mathcal{P}$*.*

In the case of shallow networks, i.e. when $L = 2$, we prove that the maximal honest open has even a nicer structure, in fact:

Proposition 5. *Let* $L = 2$*, then the maximal honest open is a Zariski open subset of* $\mathcal{P}$*.*

Conclusion

We finally summarize the impact of our results and possible future research.

We think that studying the linear descriptions B_ϕ and how they evolve as we move along the neuromanifold $\mathcal{M}_\mathbf{n}$ is a viable future route towards deeper understanding of the structure of $\mathcal{M}_\mathbf{n}$. With these tools we are currently studying the closedness of $\mathcal{M}_\mathbf{n}$.

Theorem 3 tells us that the $\mathcal{M}_\mathbf{n}$ cannot be given the structure of a semi-algebraic set in the most straightforward way. The study of singular points and other geometric features of $\mathcal{M}_\mathbf{n}$ might thus have to be carried out without the direct help of (standard) algebraic geometry. Nevertheless, even though a notion of semi-algebraic subset has never been given for an infinite dimensional space such as PL, we hint that the neuromanifold should be a *pro-semi-algebraic* space, i.e. a categorical limit of the semi-algebraic spaces studied in [1] (each of which lies inside a finite dimensional ambient space). This last consideration might have also practical relevance in the experimental study of the neuromanifold.

Having a precise knowledge about hidden and permutation/scaling symmetries for specific classes of NNs can lead to more efficient algorithms for training, among other advantages (see [3] and references therein). In our work, by introducing honest open subsets of the space of parameters, we phrase this quest in algebro-geometric terms, allowing the use of a plethora of new tools.

Acknowledgements. The first author acknowledges support from the Wallenberg AI, Autonomous Systems and Software Program (WASP) funded by the Knut and Alice Wallenberg Foundation. The second author was partially supported by the Wallenberg AI, Autonomous Systems and Software Program (WASP) funded by the Knut and Alice Wallenberg Foundation.

References

[1] Y. Alexandr, G. Montúfar: Constraining the outputs of ReLU neural networks. *ArXiv:2508.03867* (2025).

[2] G. Cybenko: Approximation by superpositions of a sigmoidal function. *Math. Control Signals Systems* **2**(4), 303–314 (1989).

[3] J.E. Grigsby, K. Lindsey, D. Rolnick: *Hidden symmetries of ReLU networks*. Proceedings of the 40th International Conference on Machine Learning PMLR **202**, 11734–11760 (2023).

[4] J. Grzybowski: Minimal pairs of convex compact sets. *Arch. Math.* **63**(2), 173–181 (1994).

[5] K. Kohn, T. Merkh, G. Montúfar, M. Trager: Geometry of linear convolutional networks. *SIAM J. Appl. Algebra Geom.* **6**(3), 368–406 (2022).

[6] K. Kohn, G. Montúfar, V. Shahverdi, M. Trager: Function space and critical points of linear convolutional networks. *SIAM J. Appl. Algebra Geom.* **8**(2), 333–362 (2024).

[7] G.L. Marchetti, V. Shahverdi, S. Mereta, M. Trager, K. Kohn: *Algebra unveils deep learning – an invitation to neuroalgebraic geometry*. Forty-second International Conference on Machine Learning (2025).

[8] M. Masden: Algorithmic determination of the combinatorial structure of the linear regions of ReLU neural networks. *SIAM J. Appl. Algebra Geom.* **9**(2), 374–404 (2025).

[9] S. Scholtes: Minimal pairs of convex bodies in two dimensions. *Mathematika* **39**(2), 267–273 (1992).

[10] V. Shahverdi, G.L. Marchetti, K. Kohn: On the geometry and optimization of polynomial convolutional networks. *ArXiv:2410.00722* (2024).

[11] C. Scheiderer: Quotients of semialgebraic spaces. *Math. Z.* **201**, 249–271 (1989).

[12] G. Smyrnis, P. Maragos: Tropical polynomial division and neural networks. *ArXiv:1911.12922* (2019).

[13] M. Trager, K. Kohn, J. Bruna: Pure and spurious critical points: a geometric study of linear networks. *ArXiv:1910.01671* (2019).

[14] N.M. Tran, J. Wang: Minimal representations of tropical rational functions. *Algebraic Statist.* **15**(1), 27–59 (2024).

[15] R. Urbański: On minimal convex pairs of convex compact sets. *Arch. Math.* **67**(3), 226–238 (1996).

[16] J. Vallin, K. Larsson, M.G. Larson: The geometric structure of fully-connected ReLU layers. *ArXiv:2310.03482* (2023).

[17] L. Zhang, G. Naitzat, L.H. Lim: *Tropical geometry of deep neural networks*. International Conference on Machine Learning PMLR, 5824–5832 (2018).

Concentration on some families of numerical semigroups

E.R. García Barroso*, W.G. Hernández-Yanes◇*
◇ *Speaker at EACA 2026*
* *University of La Laguna*
ergarcia@ull.es, whernany@ull.edu.es

Abstract. The concentration of a numerical semigroup S is defined as

$$C(S) = \max\{\text{next}_S(s) - s : s \in S \setminus \{0\}\},$$

where, for any $s \in S$, $\text{next}_S(s) = \min\{x \in S : x > s\}$. The notion of concentration of a numerical semigroup was introduced in [2], where numerical semigroups with concentration equal to 2 were completely characterized. These results were later extended in [3] to numerical semigroups with arbitrary concentration. In this talk, we present a key theorem that provides an explicit formula to compute the concentration of a numerical semigroup from its minimal system of generators. Moreover, we show that this formula can be further simplified in the case of numerical semigroups with maximal embedding dimension. Finally, we study the behavior of the concentration under the gluing of a numerical semigroup with $\mathbb{N}$.

This work, still in progress, is joint with Evelia R. García Barroso.

Numerical semigroups

A *numerical semigroup* is a subset S of $\mathbb{N}$ that is closed under the usual addition in $\mathbb{N}$, contains 0, and has finite complement in $\mathbb{N}$. One of the basic structural properties of numerical semigroups is that they are finitely generated. More precisely, let $A \subset S$ be a finite subset such that $S = \langle A \rangle$, where

$$\langle A \rangle := \{a_1\lambda_1 + \cdots + a_n\lambda_n : n \in \mathbb{N},\ \lambda_i \in \mathbb{N},\ a_i \in A,\ 1 \leq i \leq n\}.$$

Then A is called a *system of generators* of S. If no proper subset of A generates S, then A is said to be a *minimal system of generators* of S, and it is denoted by $msg(S)$.

It is well known that a submonoid $S \subset \mathbb{N}$ with $0 \in S$ is a numerical semigroup if and only if there exists a finite subset $A \subset S$ such that $S = \langle A \rangle$ and $\gcd(A) = 1$ (see, for instance, [4]). The smallest positive element of a numerical semigroup S is called its *multiplicity* and is denoted by $m(S)$. Moreover, the cardinality of $msg(S)$ is known as the *embedding dimension* of S and is denoted by $e(S)$.

J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, V. Sotomayor (eds.): Proceedings of the XIX EACA, pp. 136-140 (2026).
ISBN: 978-84-09-87277-0

Given a numerical semigroup S, the set of its *gaps* is defined as $G(S) = \mathbb{N} \setminus S$. The cardinality of $G(S)$ is called the *genus* of S and is denoted by $g(S)$. The maximum element of $G(S)$ is known as the *Frobenius number* of S, denoted by $F(S)$, with the convention that $F(\mathbb{N}) = -1$.

Finally, a numerical semigroup S whose minimal system of generators is of the form

$$msg(S) = \{m, m+1, \ldots, m+k\},$$

for some $k \in \{1, \ldots, m-1\}$, is called a *quasi half-line* or a *quasi ordinary* semigroup. When $k = m-1$, we say that S is a *half-line* or an *ordinary* semigroup; in this case, $S = \{0, m, \rightarrow\}$.

Concentration of a numerical semigroup

Let S be a numerical semigroup. For any $s \in S \setminus \{0\}$, we denote by

$$\mathsf{next}_S(s) = \mathsf{min}\{x \in S : s < x\}$$

the next element of S after s. The *concentration* of S is defined as

$$C(S) = \mathsf{max}\{\mathsf{next}_S(s) - s : s \in S \setminus \{0\}\}.$$

A numerical semigroup S satisfies $C(S) = 1$ if and only if S is a half-line numerical semigroup.

The following result gives an upper bound for the concentration of a numerical semigroup in terms of its multiplicity.

Proposition 1. *Let S be a numerical semigroup and let $m(S)$ be its multiplicity. Then*

$$C(S) \leq m(S).$$

We can characterize when a semigroup attains its maximum concentration.

Proposition 2. *Let S be a numerical semigroup with multiplicity m. Then S has maximum concentration if and only if*

$$\mathit{next}_S(m) = 2m.$$

The next theorem provides an explicit formula to compute the concentration from the minimal system of generators.

Theorem 3. *Let S be a numerical semigroup with $msg(S) = \{v_0, \ldots, v_h\}$, and let*

$$i_C := \mathsf{max}\{i \in \{0, \ldots, h\} : v_i < 2v_0\}.$$

Define $\tilde{v}_k = v_k$ for all $k \in \{0, \ldots, i_C\}$ and $\tilde{v}_{i_C+1} = 2v_0$. Then

$$C(S) = \max_{0 \leq k \leq i_C} \{\tilde{v}_{k+1} - \tilde{v}_k\}.$$

For semigroups generated by two elements, the concentration can be computed directly as follows.

Corollary 4. *Let $S = \langle a, b\rangle$ be a numerical semigroup with embedding dimension 2. Then*

$$C(S) = \begin{cases} \max\{2a - b,\ b - a\}, & \text{if } 2a > b, \\ a, & \text{if } 2a < b. \end{cases}$$

Quasi half-line semigroups have a simple formula for the concentration.

Corollary 5. *Let S be a quasi half-line numerical semigroup with $msg(S) = \{m, m + 1, \ldots, m + k\}$. Then*

$$C(S) = m - k.$$

Gluing of numerical semigroups

Let S be a numerical semigroup with minimal system of generators $msg(S) = \{v_0, \ldots, v_h\}$. Let $d \in \mathbb{N} \setminus \{0, 1\}$ and $\gamma \in S \setminus \{v_0, \ldots, v_h\}$ be such that $\gcd(d, \gamma) = 1$. The numerical semigroup

$$S \oplus_{d,\gamma} \mathbb{N} := \mathbb{N}dv_0 + \cdots + \mathbb{N}dv_h + \mathbb{N}\gamma$$

is called the *gluing of S and $\mathbb{N}$ with respect to (d, γ)*.

The following proposition shows how the concentration behaves under gluing when the original semigroup has maximum concentration.

Proposition 6. *Let S be a numerical semigroup with maximum concentration and $msg(S) = \{v_0, \ldots, v_h\}$. Then*

$$C(S \oplus_{d,\gamma} \mathbb{N}) = d\, C(S)$$

if and only if $\gamma > 2dv_0$.

Let us fix the notation

$$I_C := \{k \in \{0, \ldots, i_C\} : C(S) = \tilde{v}_{k+1} - \tilde{v}_k\},\ k_C := \min(I_C).$$

The next result provides a characterization of the concentration under gluing in the case where the maximum concentration is attained by more than one difference.

Proposition 7. *Let S be a numerical semigroup with $msg(S) = \{v_0, \ldots, v_h\}$, $C(S) < v_0$ and $|I_C| > 1$. Then*

$$C(S \oplus_{d,\gamma} \mathbb{N}) = d\, C(S) \quad \text{if and only if} \quad 2\gamma > d\tilde{v}_{k_C+1}.$$

Half-line semigroups under gluing satisfy the following simple criterion.

Corollary 8. *Let S be a half-line numerical semigroup with multiplicity m. Then*

$$C(S \oplus_{d,\gamma} \mathbb{N}) = d \quad \text{if and only if} \quad 2\gamma > dm.$$

When the concentration is attained at a single difference, its behavior under gluing can be described as follows.

Proposition 9. *Let S be a numerical semigroup with $msg(S) = \{v_0, \dots, v_h\}$, $C(S) < v_0$ and $|I_C| = 1$. Then*

$$C(S \oplus_{d,\gamma} \mathbb{N}) = d\,C(S)$$

if and only if

$$\gamma \in \left(\left(\tfrac{d\tilde{v}_{k_C+1}}{2},\, d\tilde{v}_{k_C}\right) \cup \left(d\tilde{v}_{k_C+1}, +\infty\right)\right) \cap S.$$

The concentration for quasi half-line semigroups under gluing follows this rule.

Corollary 10. *Let S be a quasi half-line numerical semigroup with multiplicity m. Then*

$$C(S \oplus_{d,\gamma} \mathbb{N}) = d(m-k)$$

if and only if

$$\gamma \in \left(\left(\tfrac{d(m+k)}{2},\, d(m+k)\right) \cup (2dm, +\infty)\right) \cap S.$$

SI-SEMIGROUPS

A sequence of positive integers $(v_0, \dots, v_h)$ is called a *characteristic sequence* if, letting $e_k = \gcd(v_0, \dots, v_k)$ for $0 \le k \le h$, one has $e_k < e_{k-1}$ for all $1 \le k \le h$, $e_h = 1$, and $e_{k-1}v_k < e_k v_{k+1}$ for all $1 \le k \le h-1$. A numerical semigroup is said to be *strongly increasing* (SI) if it is generated by a characteristic sequence.

It is well known that all SI-semigroups are obtained by gluing. The concentration of this family of semigroups is simply scaled by d.

Corollary 11. *Let $\overline{S} = S \oplus_{d,\gamma} \mathbb{N}$ be an SI-semigroup. Then*

$$C(\overline{S}) = d\,C(S).$$

For SI-semigroups, the concentration depends only on the first two minimal generators.

Corollary 12. *Let S be an SI-semigroup with $msg(S) = \{v_0, \dots, v_h\}$. Then*

$$C(S) = \begin{cases} \max\{2v_0 - v_1,\ v_1 - v_0\}, & \text{if } 2v_0 > v_1, \\ v_0, & \text{if } 2v_0 < v_1. \end{cases}$$

On the other hand, it is well known that numerical semigroups associated with plane branches are SI-semigroups, and we also provide a geometric interpretation of this fact.

REFERENCES

[1] M. Delgado, P.A. García-Sánchez, J.J. Morais: *NumericalSgps, a package for numerical semigroups*. Version 1.4.0. `https://gap-packages.github.io/numericalsgps/doc/chap0_mj.html`

[2] J.C. Rosales, M.B. Branco, M.A. Traesel: Numerical semigroups with concentration two. *Indag. Math. (N.S.)* **33**(2), 303–313 (2022).

[3] J.C. Rosales, M.B. Branco, M.A. Traesel: Numerical semigroups with fixed multiplicity and concentration. *J. Commut. Algebra* **17**(1), 63–74 (2025).

[4] J.C. Rosales, P.A. García-Sánchez: *Numerical semigroups*. Developments in Mathematics **20**, Springer (2009).

[5] The GAP Group: *GAP - Groups, Algorithms, and Programming*. Version 4.14.0. `https://www.gap-system.org` (2024)

Posets of trek polynomials in directed acyclic graphs

M. Garrote-López[◇*], N. Kushnerchuk[†], L. Solus[‡]

[◇] *Speaker at EACA 2026*

[*] *Universitat Pompeu Fabra*

[†] *Aalto University*

[‡] *KTH Royal Institute of Technology*

marina.garrote@upf.edu, nataliia.kushnerchuk@aalto.fi, solus@kth.se

Abstract. We associate a graphical model (semialgebraic set) to each directed acyclic graph. A key problem is comparing these models to determine when they are distinguishable. We address this by studying the minimal linear subspaces containing them. We introduce a poset associated to a graph and use its properties to describe these subspaces. The analysis reveals connections to Young tableaux, Ehrhart theory, and toric ideals.

Introduction

Let $\mathcal{G} = ([m], E)$ be a directed acyclic graph (DAG) with nodes $[m] = \{1, \ldots, m\}$ and edges E. We introduce a partially order set (poset) $P_{\mathcal{G}}$ associated to $\mathcal{G}$ whose combinatorial invariants can be used to compute the linear span of a semialgebraic set $\mathcal{M}(\mathcal{G}) \subset \mathbb{R}^{m \times m}$ associated to $\mathcal{G}$. The set $\mathcal{M}(\mathcal{G})$ arises in statistics in the context of linear structural equation models. It consists of covariance matrices parameterizing distributions over Gaussian random variables $X_1, \ldots, X_m$ associated to the nodes of $\mathcal{G}$ where linear dependences between X_i are modeled by the edges in $\mathcal{G}$. However, it is possible that $\mathcal{M}(\mathcal{G}) = \mathcal{M}(\mathcal{H})$, despite being defined by different DAGs $\mathcal{G} \neq \mathcal{H}$. This leads to a fundamental identifiability problem: For which DAGs $\mathcal{G}, \mathcal{H}$ do we obtain distinct semialgebraic sets $\mathcal{M}(\mathcal{G}) \neq \mathcal{M}(\mathcal{H})$?

A simple certificate for distinguishing two sets, is a linear polynomial f satisfying $f(x) = 0$ for all points $x \in \mathcal{M}(\mathcal{G})$ and $f(y) \neq 0$ for some $y \in \mathcal{M}(\mathcal{H})$. This motivates the identification of the linear span of these semialgebraic sets. Interestingly, the solution to this problem is combinatorial, relying on the combinatorics of certain posets $P_{\mathcal{G}}$ associated to $\mathcal{M}(\mathcal{G})$. We show that this basis can be computed with the help of the Möbius function of $P_{\mathcal{G}}$ and the theory of P-partitions. Along the way, we point out connections that emerge to other areas of interest in combinatorics.

Trek polynomials and semialgebraic sets for DAGs

Let $\mathcal{G} = ([m], E)$ be a DAG. Statistically, a directed path $P = \{v_1 \to v_2, v_2 \to v_3, \ldots, v_{k-1} \to v_k\}$ represents a pathway where X_{v_1} has an (indirect) effect on X_{v_k}. If

J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, V. Sotomayor (eds.): Proceedings of the XIX EACA, pp. 141-145 (2026).
ISBN: 978-84-09-87277-0

a second path $Q = \{v_1 \to w_2, \dots, w_{\ell-1} \to w_\ell\}$ exists, the pair (P, Q) represents a correlation between X_{w_ℓ} and X_{v_k} induced by their common cause X_{v_1}: $w_\ell \leftarrow w_{\ell-1} \leftarrow \cdots \leftarrow w_2 \leftarrow v_1 \to v_2 \to \cdots \to v_{k-1} \to v_k$. The pair of paths $T = (P, Q)$ is a *trek* (between v_k and w_ℓ), and v_1 is the *top* of T, denoted $\mathrm{top}(T)$. We denote the set of all treks between $i, j \in [m]$ as $\mathcal{T}(i, j)$. A trek is *simple* (set $\mathcal{S}(i, j)$) if it has no repeated vertices.

To every edge $i \to j \in E$, associate a parameter λ_{ij} (representing the direct effect of i on j), and to each node $k \in [m]$ a parameter ω_k (representing the variance of the independent Gaussian error term at k). Given a trek $T = (P, Q) \in \mathcal{T}(i, j)$, define the *trek monomial*: $m_T = \omega_{\mathrm{top}(T)} \prod_{k \to \ell \in P} \lambda_{k\ell} \prod_{k \to \ell \in Q} \lambda_{k\ell}$. The *trek polynomial* $p_{i,j}$ parametrizes the covariance entry $\Sigma_{i,j}$ between X_i and X_j:

$$p_{i,j} = \sum_{T \in \mathcal{T}(i,j)} m_T. \tag{1}$$

Colored Gaussian DAG models

A *coloring* of a DAG $\mathcal{G} = ([m], E)$ consists of surjective maps $c_E : E \to [e]$ and $c_V : [m] \to [n]$. The *colored trek polynomials* are obtained by specializing parameters in (1) via the coloring: $\lambda_{ij} \mapsto \lambda_{c_E(ij)}$ and $\omega_i \mapsto \omega_{c_V(i)}$. This defines a polynomial map

$$\varphi_{\mathcal{G},c} : \mathbb{R}^e \times \mathbb{R}^n_{>0} \to \mathbb{R}^{m \times m}, \quad (\lambda, \omega) \mapsto (\Sigma_{ij})_{i,j=1}^m.$$

The image is a semialgebraic set $\mathcal{M}(\mathcal{G}, c)$, the *colored Gaussian DAG model* [1]. A central question is *distinguishability*: for which pairs is $\mathcal{M}(\mathcal{G}, c) \neq \mathcal{M}(\mathcal{H}, c')$?

We focus on distinguishing models via linear invariants. Let $\mathcal{T}$ be the set of unique trek monomials generated by $(\mathcal{G}, c)$. We define $M_{\mathcal{G},c}$ as the matrix where rows are indexed by pairs $\{i, j\}$ and columns by monomials $m \in \mathcal{T}$. The entry $(M_{\mathcal{G},c})_{\{i,j\},m}$ counts the number of treks in $\mathcal{T}(i, j)$ with monomial m. Identifying covariance matrices with their vectors of unique entries, the map $\varphi_{\mathcal{G},c}$ factors linearly as $\varphi_{\mathcal{G},c}(\cdot) = M_{\mathcal{G},c} \cdot \mathbf{v}(\lambda, \omega)$, where $\mathbf{v}$ is the vector of monomials. Consequently, the linear forms vanishing on the model are exactly $\ker(M^t_{\mathcal{G},c})$. Our goal is to compute a basis for $\ker(M^t_{\mathcal{G},c})$. We solve this by associating a poset $P_{\mathcal{G},c}$ to the matrix and analyzing its Möbius function and combinatorial properties.

Posets on trek polynomials

We now introduce a poset structure to systematically find linear invariants for colored DAG models. For any pair of nodes i, j, let $t(i, j) \in \mathbb{N}^{\mathcal{T}}$ be the vector where the m-th coordinate counts the number of treks in $\mathcal{T}(i, j)$ with monomial m. We define a meet operation on these vectors by component-wise minimum: $u \wedge v := (\min(u_m, v_m) : m \in \mathcal{T})$. Let $P_{\mathcal{G},c}$ be the poset with ground set the set of all finite meets of the vectors $\{t(i, j) : i, j \in [m]\}$, ordered by component-wise domination ($t \preceq s \iff t_m \leq s_m$). We show that the poset $P_{\mathcal{G},c}$ is a meet-semilattice with a unique minimal element $\hat{0} = 0$.

Our goal is to relate $P_{\mathcal{G},c}$ to the algebraic constraints of the model. Define the evaluation map $g(s) = \sum_{m \in \mathcal{T}} s_m \cdot m$. Note that if $s = t(i, j)$, then $g(s)$ corresponds to the model covariance σ_{ij}. Using the Möbius inversion formula [5] on $P_{\mathcal{G},c}$, we define a polynomial $f(s)$:

Theorem 1. *For any element $s \in P_{\mathcal{G},c}$, define $f(s) = s - \bigvee_{s' \prec s} s'$ for $s \in P_{\mathcal{G},c}$, where $s \vee s' = (\max(s_m, s'_m) : m \in \mathcal{T})$. Then $f(s) = \sum_{t \preceq s} \mu(t,s) g(t)$.*

Note that, when $f(s)$ vanishes on the parameter space $\mathbb{R}^e \times \mathbb{R}^n_{>0}$ of $\mathcal{M}(G,c)$, we obtain a linear constraint $0 = f(s) = \sum_{s' \preceq s} \mu(s',s) g(s')$. As an example, the combinatorics of which (uncolored) DAG models can be distinguished by their *marginal independences* (i.e. $\sigma_{ij} = 0$) is well-understood [2]. Theorem 1 provides a generalization of these constraints to the colored DAG models $\mathcal{M}(\mathcal{G},c)$ for any coloring. The following lemma characterizes exactly when this vanishing occurs, reducing the algebraic problem to a combinatorial one.

Lemma 2. *$f(s)$ is identically zero on the model $\mathcal{M}(\mathcal{G},c)$ if and only if $s = \bigvee_{t \in \text{lower}(s)} t$. In particular, if the lower cover of s has size ≥ 2, we obtain a linear invariant.*

Thus, to distinguish models, we need only compute the poset $P_{\mathcal{G},c}$ and identify elements that are the join of their lower covers.

π-GRAPHS AND P-PARTITIONS FOR POLYTREES

We focus on polytrees $\mathcal{G}$ (DAGs whose underlying undirected graph is a tree) with constant coloring c^*, where we set $\lambda = \lambda_{ij}$ for all $i \to j \in E$ and $\omega_k = 1$ for all $k \in [m]$.

Trek polynomials from polytrees

In a polytree, any trek between i and j factors uniquely into a simple trek S_{ij} and a set of is a self-trek between $\text{top}(S_{ij})$ and itself. We define the *ancestral polynomial* of a node k in $\mathcal{G}$ as $A_k(\lambda) = \sum_{a \in \text{an}_\mathcal{G}(k)} \lambda^{d(a,k)}$, where $\text{an}_\mathcal{G}(k)$ denote the ancestors of k, and $d(a,k)$ the distance from a to k. This factorization yields to:

Proposition 3. *Let $\mathcal{G}$ be a polytree. Then $p_{i,j}(\lambda) = \lambda^{|S_{ij}|} A_{\text{top}(S_{ij})}(\lambda^2)$. Furthermore, if $\mathcal{G}$ is a directed tree (polytree with a single source node) rooted at r, the ancestral polynomial simplifies to a geometric series: $A_k(\lambda) = 1 + \lambda^2 + \cdots + \lambda^{2d(r,k)}$.*

For general polytrees we have that $A_k(\lambda) = 1 + \sum_{j \geq 1} c_j \lambda^{2j}$ where $c(k) = (c_1, c_2, \ldots)$ is the *content* of a node k in $\mathcal{G}$. Then, trek polynomials are of the form $p = \lambda^w \left(1 + \sum_{j \geq 1} c_j \lambda^{2j}\right)$ and we call $w = w(p)$ the *width* of p and $c = c(p)$ its *content*. Combinatorially, the content c of k counts the number of edges at successive levels that point toward k. These content vectors relate to "tree-like fillings" of Young diagrams, a connection we omit here for brevity.

π-graphs

The invariants derived from the Möbius inversion formula in Theorem 1 provide linear invariants when the evaluation $g(s)$ corresponds directly to a model coordinate σ_{ij}. This occurs when the poset elements are realizable as trek vectors.

Definition 4. A colored DAG $(\mathcal{G}, c)$ is a π-*graph* if the ground set of $P_{\mathcal{G},c}$ is exactly $\mathbb{M}_{\mathcal{G},c} = \{t(i,j) : i,j \in [m]\} \cup \{0\}$. Equivalently, the set of vectors $\{t(i,j)\}$ forms a π-system (it is closed under intersection).

Finite π-systems are closely related to finite topologies, which are known to be difficult to enumerate [3]. Moreover, being a π-graph is a sufficient condition to guarantee that the inversion formula (Theorem 1) will yield linear constraints satisfied by the model $\mathcal{M}(G, c)$ whenever $f(s) = 0$. This motivates characterizing the colored DAGs $(\mathcal{G}, c)$ that are π-graphs, which we do for directed trees and standard polytrees (omited in this abstract) under the constant coloring c^*.

In this setting, we consider the poset $\mathcal{C}_\mathcal{G}$ with ground set the content vectors $c(k)$, or equivalently $c(p_{i,j})$. We define a natural partial order on contents: $c \preceq c'$ iff $c_k \leq c'_k$ for all k. We also define the *width function* by $w_\mathcal{G}(c) = \max\{w(p) : a \in \mathbb{M}_{(\mathcal{G},c^*)} \text{ and } c(p) = c\}$.

Theorem 5. *Let $\mathcal{G}$ be a directed tree with constant coloring c^*. Then $(\mathcal{G}, c^*)$ is a π-graph if and only if $w_\mathcal{G}$ is a P-partition of $\mathcal{C}_\mathcal{G}$ (i.e., $c \preceq c' \implies w_\mathcal{G}(c) \geq w_\mathcal{G}(c')$).*

The set of valid width functions corresponds to lattice points in an order polytope, linking this problem to Ehrhart theory [4]. We also prove that for general polytrees, requiring $\mathcal{C}_\mathcal{G}$ to be a π-system is a necessary condition for $(\mathcal{G}, c^*)$ to be a π-graph.

Linear invariants of directed trees

For directed trees satisfying the condition of Theorem 5, we can fully solve the distinguishability problem. Since $(\mathcal{G}, c^*)$ is a π-graph, the Möbius function on $P_{\mathcal{G},c^*}$ is straightforward. The condition $f(s) = 0$ holds if and only if s covers exactly two elements s_1, s_2. The relation $s - s_1 - s_2 + (s_1 \wedge s_2) = 0$ in the poset translates to the linear tetrad constraint:

$$\sigma_{ij} - \sigma_{k\ell} - \sigma_{uv} + \sigma_{wz} = 0, \tag{2}$$

where $t(i,j) = s$, $t(k,\ell) = s_1$, $t(u,v) = s_2$, and $t(w,z) = s_1 \wedge s_2$.

Theorem 6. *Let $\mathcal{G}$ be a directed tree with constant coloring c^*, then we have the following:*
(1) Basis: *The linear ideal of $\mathcal{M}(\mathcal{G}, c^*)$ is generated by equalities $\sigma_{ij} - \sigma_{kl}$ where $t(i,j) = t(k,l)$, and the tetrad constraints* (2) *for all s with $f(s) = 0$.*
(2) Dimension: *The dimension of the linear span is $2h(\mathcal{G}) + 1$, where $h(\mathcal{G})$ is the length of the longest path.*
(3) Toric Geometry: *The variety $\overline{\mathcal{M}(\mathcal{G}, c^*)}$ is toric. Given the poset $P_{\mathcal{G},c^*}$, there exists a linear change of variables that renders the parametrization monomial. Using this coordinate change and the structure of $P_{\mathcal{G},c^*}$, we derive a full description of the binomial generators of the toric ideal defining the variety.*
(4) Reconstruction and distinguishability: *We propose an explicit algorithm to recover the poset $P_{\mathcal{G},c^*}$ and the graph $\mathcal{G}$ from the linear constraints. Consequently,* $\ker(M_{\mathcal{G},c^*}) = \ker(M_{\mathcal{H},c^*})$ *implies $\mathcal{G} \cong \mathcal{H}$.*

In summary, we introduce a poset-theoretic framework that solves the distinguishability problem for some families of colored DAGs. We demonstrate that the linear variety uniquely

determines the graph and poset, while the poset structure explicitly encodes the toric generators. This establishes a robust dictionary between the combinatorics of P-partitions and the algebraic geometry of graphical models.

Acknowledgements. The first author was partially supported by the Wallenberg Autonomous Systems and Software Program (WASP) funded by the Knut and Alice Wallenberg Foundation and by the Beatriu de Pinós postdoctoral programme of the Department of Research and Universities of the Generalitat de Catalunya (ref. 2024BP00235). The second author was partially supported by the Foundation for Aalto University Science and Technology. The third author was partially supported by the WASP funded by the Knut and Alice Wallenberg Foundation, a Starting Grant from the Swedish Research Council (Vetenskapsrådet), the Göran Gustafsson Foundation's Prize for Young Researchers, and a Research Pairs Grant from the Center for Digital Futures at KTH.

References

[1] T. Boege, K. Kubjas, P. Misra, L. Solus: Colored Gaussian DAG models. *J. R. Stat. Soc. Ser. B. Stat. Methodol.* (2025).

[2] D. Deligeorgaki, A. Markham, P. Misra, L. Solus: Combinatorial and algebraic perspectives on the marginal independence structure of Bayesian networks. *Algebraic Statist.* **14**(2), 233–286 (2024).

[3] D.J. Kleitman, B.L. Rothschild: Asymptotic enumeration of partial orders on a finite set. *Trans. Amer. Math. Soc.* **205**, 205–220 (1975).

[4] R.P. Stanley: Two poset polytopes. *Discrete Comput. Geom.* **1**(1), 9–23 (1986).

[5] R.P. Stanley: *Enumerative Combinatorics.* 2nd ed., Cambridge Studies in Advanced Mathematics, Cambridge University Press (2011).

On Hopf braces and crossed products

R. González Rodríguez*, B. Ramos Pérez◇†

◇ *Speaker at EACA 2026*

* *Department of Applied Mathematics II, I.S. Telecommunication, University of Vigo*

† *Department of Mathematics, Faculty of Mathematics, University of Santiago de Compostela*

rgon@dma.uvigo.es, braisramos.perez@usc.es

Abstract. In this presentation we describe the progress made towards the solution of the following problem: If $\mathbb{A} = (A_1, A_2)$ and $\mathbb{H} = (H_1, H_2)$ are Hopf braces in a symmetric monoidal category C such that (A_1, H_1) and (A_2, H_2) are matched pairs of Hopf algebras, then we want to know under what conditions the pair $(A_1 \bowtie H_1, A_2 \bowtie H_2)$ constitutes a new Hopf brace. We find such conditions for the pairs of Hopf algebras $(A_1 \otimes H_1, A_2 \bowtie H_2)$ and $(A_1 \bowtie H_1, A_2 \sharp H_2)$ to be Hopf braces, which are particular situations of the general problem described above, analyzing when these are cocommutative, leading to solutions to the Quantum Yang-Baxter equation. These results are applied to study when the Drinfeld Double gives rise to a Hopf brace. The novel results presented in this presentation can be found in [5].

Introduction

A Hopf brace is a recent mathematical object introduced by I. Angiono, C. Galindo and L. Vendramin in [1] which was born as the quantum version of a skew brace. As a generalization of W. Rump's braces [8], skew braces appeared in [6] in order to study non-degenerate solutions to the Quantum Yang-Baxter equation.

Throughout this presentation we will be working in a strict symmetric monoidal setting. For us C will denote a strict symmetric monoidal category with tensor product $\otimes$, unit object K and natural isomorphism of symmetry c. In this presentation we will use the notation $P \otimes f$ and $f \otimes P$ to refer to $id_P \otimes f$ and $f \otimes id_P$, respectively, for all morphisms $f\colon M \to N$ in C and for all P object in C. In this categorical framework, a Hopf brace is defined as follows:

Definition 1. Let $(H, \varepsilon_H, \delta_H)$ be a coalgebra in C and let us assume that H admits two different algebra structures in C: (H, η_H^1, μ_H^1) and (H, η_H^2, μ_H^2). We will say that a 9-tuple $(H, \eta_H^1, \mu_H^1, \eta_H^2, \mu_H^2, \varepsilon_H, \delta_H, \lambda_H^1, \lambda_H^2)$ is a Hopf brace in C if the following requirements hold:

(i) $H_1 = (H, \eta_H^1, \mu_H^1, \varepsilon_H, \delta_H, \lambda_H^1)$ is a Hopf algebra in C.

(ii) $H_2 = (H, \eta_H^2, \mu_H^2, \varepsilon_H, \delta_H, \lambda_H^2)$ is a Hopf algebra in C.

J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, V. Sotomayor (eds.): Proceedings of the XIX EACA, pp. 146-150 (2026).
ISBN: 978-84-09-87277-0

(iii) The following identity involving the products μ_H^1 and μ_H^2 holds:

$$\mu_H^2 \circ (H \otimes \mu_H^1) = \mu_H^1 \circ (\mu_H^2 \otimes \Gamma_{H_1}) \circ (H \otimes c_{H,H} \otimes H) \circ (\delta_H \otimes H \otimes H),$$

where $\Gamma_{H_1} \coloneqq \mu_H^1 \circ (\lambda_H^1 \otimes \mu_H^2) \circ (\delta_H \otimes H)$.

Following the notation introduced in [3], we will denote Hopf braces by $\mathbb{H} = (H_1, H_2)$ or, when there is no confusion between the Hopf algebras involved, only by $\mathbb{H}$. A Hopf brace $\mathbb{H}$ is said to be cocommutative if the underlying coalgebra structure, $(H, \varepsilon_H, \delta_H)$, is cocommutative, that is to say, if $c_{H,H} \circ \delta_H = \delta_H$.

Given a Hopf brace $\mathbb{H} = (H_1, H_2)$, note that $\eta_H^1 = \eta_H^2$ [1, Remark 1.3]. Therefore, from now on we will denote both units by η_H. Moreover, (H_1, Γ_{H_1}) is a left H_2-module algebra as was proved in [1, Lemma 1.8]. By naturality of c, coassociativity of δ_H and associativity of μ_H^1,

$$\begin{aligned}&\mu_H^1 \circ (\mu_H^2 \otimes \Gamma_{H_1}) \circ (H \otimes c_{H,H} \otimes H) \circ (\delta_H \otimes H \otimes H)\\ =&\mu_H^1 \circ (\Gamma'_{H_1} \otimes \mu_H^2) \circ (H \otimes c_{H,H} \otimes H) \circ (\delta_H \otimes H \otimes H),\end{aligned}$$

where $\Gamma'_{H_1} \coloneqq \mu_H^1 \circ (\mu_H^2 \otimes \lambda_H^1) \circ (H \otimes c_{H,H}) \circ (\delta_H \otimes H)$. Therefore, condition (iii) of Definition 1 is equivalent to

$$\mu_H^2 \circ (H \otimes \mu_H^1) = \mu_H^1 \circ (\Gamma'_{H_1} \otimes \mu_H^2) \circ (H \otimes c_{H,H} \otimes H) \circ (\delta_H \otimes H \otimes H).$$

It is important to recall that, under the cocommutativity hypothesis, H is also a right H_2-module coalgebra with the action given by

$$\Phi_H \coloneqq \mu_H^2 \circ ((\lambda_H^2 \circ \Gamma_{H_1}) \otimes \mu_H^2) \circ (H \otimes c_{H,H} \otimes H) \circ (\delta_H \otimes \delta_H),$$

a result whose proof can be seen in [1, Lemma 2.2]. In addition, if $\mathbb{H} = (H_1, H_2)$ is a cocommutative Hopf brace, then the morphism

$$\tau = (\Gamma_{H_1} \otimes \Phi_H) \circ (H \otimes c_{H,H} \otimes H) \circ (\delta_H \otimes \delta_H) \tag{1}$$

is a solution to the Quantum Yang-Baxter equation [1, Corollary 2.4].

Description of the problem and main results

In this presentation the construction of the bicrossed product Hopf algebra from a matched pair will play a central role.

Definition 2. Let H and A be Hopf algebras in C. A 4-tuple $(A, H, \varphi_A, \phi_H)$ is said to be a matched pair of Hopf algebras if the following conditions hold:

(i) (A, φ_A) is a left H-module coalgebra and (H, ϕ_H) is a right A-module coalgebra,

(ii) $\varphi_A \circ (H \otimes \eta_A) = \varepsilon_H \otimes \eta_A$, i.e., η_A is a morphism of left H-modules,

(iii) $\phi_H \circ (\eta_H \otimes A) = \eta_H \otimes \varepsilon_A$, i.e., η_H is a morphism of right A-modules,

(iv) $\varphi_A \circ (H \otimes \mu_A) = \mu_A \circ (A \otimes \varphi_A) \circ (\Psi \otimes A)$,

(v) $\phi_H \circ (\mu_H \otimes A) = \mu_H \circ (\phi_H \otimes H) \circ (H \otimes \Psi)$,

(vi) $c_{A,H} \circ \Psi = (\phi_H \otimes \varphi_A) \circ (H \otimes c_{H,A} \otimes A) \circ (\delta_H \otimes \delta_A)$,

where $\Psi := (\varphi_A \otimes \phi_H) \circ (H \otimes c_{H,A} \otimes A) \circ (\delta_H \otimes \delta_A)$.

Every matched pair gives rise to a new Hopf algebra structure in the following way:

$$A \bowtie H = (A \otimes H, \eta_{A\bowtie H}, \mu_{A\bowtie H}, \varepsilon_{A\bowtie H}, \delta_{A\bowtie H}, \lambda_{A\bowtie H}),$$

where

$$\eta_{A\bowtie H} := \eta_A \otimes \eta_H, \quad \mu_{A\bowtie H} := (\mu_A \otimes \mu_H) \circ (A \otimes \Psi \otimes H), \quad \varepsilon_{A\bowtie H} := \varepsilon_A \otimes \varepsilon_H,$$
$$\delta_{A\bowtie H} := (A \otimes c_{A,H} \otimes H) \circ (\delta_A \otimes \delta_H), \quad \lambda_{A\bowtie H} := \Psi \circ (\lambda_H \otimes \lambda_A) \circ c_{A,H},$$

called the bicrossed product of A with H [7, Theorem 7.2.2].

Given $(A, H, \varphi_A, \phi_H)$ a matched pair, note that

- if $\phi_H = H \otimes \varepsilon_A$, then the bicrossed product of A with H coincides with the so-called smash product Hopf algebra of A with H, denoted by $A\sharp H$,
- if $\phi_H = H \otimes \varepsilon_A$ and $\varphi_A = \varepsilon_H \otimes A$, then the bicrossed product is the usual tensor product Hopf algebra $A \otimes H$.

Thus, we address the following problem: Let us suppose that $\mathbb{A} = (A_1, A_2)$ and $\mathbb{H} = (H_1, H_2)$ are Hopf braces in C such that $(A_1, H_1, \varphi_A^1, \phi_H^1)$ and $(A_2, H_2, \varphi_A^2, \phi_H^2)$ are matched pairs of Hopf algebras. Then

$$A_1 \bowtie H_1 = (A \otimes H, \eta_{A\otimes H}, \mu^1_{A\bowtie H}, \varepsilon_{A\otimes H}, \delta_{A\otimes H}, \lambda^1_{A\bowtie H}),$$
$$A_2 \bowtie H_2 = (A \otimes H, \eta_{A\otimes H}, \mu^2_{A\bowtie H}, \varepsilon_{A\otimes H}, \delta_{A\otimes H}, \lambda^2_{A\bowtie H})$$

are Hopf algebras in C with the same underlying coalgebra structure. So, the question we want to address is the following:

Under what conditions $(A_1 \bowtie H_1, A_2 \bowtie H_2)$ gives rise to a new Hopf brace in C? (P)

Although we did not manage to obtain a complete solution for (P), we have solved it in the following two particular cases which are close to the full solution:

Theorem 3. *Let $\mathbb{A} = (A_1, A_2)$ be a Hopf brace and $\mathbb{H} = (H_1, H_2)$ a cocommutative Hopf brace such that $(A_2, H_2, \varphi_A, \phi_H)$ is a matched pair of Hopf algebras. Under these conditions, the pair $(A_1 \otimes H_1, A_2 \bowtie H_2)$ is a Hopf brace in* C *if and only if the following conditions hold:*

(E1) $\mu_A^1 \circ (\varphi_A \otimes \varphi_A) \circ (H \otimes c_{H,A} \otimes A) \circ (\delta_H \otimes A \otimes A) = \varphi_A \circ (H \otimes \mu_A^1)$,

(E2) $\mu_H^1 \circ (\mu_H^2 \otimes \Omega) \circ (H \otimes c_{H,H} \otimes A \otimes H) \circ (((\phi_H \otimes H) \circ (H \otimes c_{H,A}) \circ (\delta_H \otimes A)) \otimes H \otimes A \otimes H)$
$= \mu_H^2 \circ ((\phi_H \circ (H \otimes \mu_A^1)) \otimes \mu_H^1) \circ (H \otimes A \otimes c_{H,A} \otimes H)$,

where $\Omega := \mu_H^1 \circ (\lambda_H^1 \otimes (\mu_H^2 \circ (\phi_H \otimes H))) \circ (\delta_H \otimes A \otimes H)$.

Consequently, in the above situation, if $\mathbb{A}$ is also a cocommutative Hopf brace and the conditions (E1) *and* (E2) *hold, then the Hopf brace $(A_1 \otimes H_1, A_2 \bowtie H_2)$ is cocommutative too, and hence a new solution to the Quantum Yang-Baxter equation is obtained via* (1).

Theorem 4. *Let $\mathbb{A} = (A_1, A_2)$ and $\mathbb{H} = (H_1, H_2)$ be Hopf braces in* C *such that*

(i) *$(A_1, H_1, \varphi_A^1, \phi_H)$ is a matched pair of Hopf algebras,*

(ii) *(A_2, φ_A^2) is a left H_2-module algebra-coalgebra satisfying*

$$(H \otimes \varphi_A^2) \circ ((c_{H,H} \circ \delta_H) \otimes A) = (H \otimes \varphi_A^2) \circ (\delta_H \otimes A).$$

The pair $(A_1 \bowtie H_1, A_2 \sharp H_2)$ is a Hopf brace in C *if and only if the next conditions hold:*

(C1) $(A \otimes \mu_H^1) \circ (\Psi^1 \otimes \mu_H^2) \circ (H \otimes \Psi^2 \otimes H) \circ (((\Gamma'_{H_1} \otimes H) \circ (H \otimes c_{H,H}) \circ (\delta_H \otimes H)) \otimes A \otimes H)$
$= (A \otimes \mu_H^2) \circ (\Psi^2 \otimes \mu_H^1) \circ (H \otimes \Psi^1 \otimes H),$

(C2) $(\Gamma_{A_1} \otimes H) \circ (A \otimes \Psi^1) = \Psi^1 \circ (H \otimes \Gamma_{A_1}) \circ (c_{A,H} \otimes A),$

(C3) $\Psi^2 \circ (H \otimes \mu_A^1) = (\mu_A^1 \otimes H) \circ (A \otimes \Psi^2) \circ (\Psi^2 \otimes A).$

Moreover, if both $\mathbb{A}$ and $\mathbb{H}$ are cocommutative Hopf braces satisfying conditions (C1), (C2) *and* (C3), *then the Hopf brace $(A_1 \bowtie H_1, A_2 \sharp H_2)$ is also a cocommutative Hopf brace giving rise to a new solution to the Quantum Yang-Baxter equation determined by* (1).

Applications to the Drinfeld Double

Y. Doi and M. Takeuchi [2] proved that the Drinfeld Double arises as a bicrossed product Hopf algebra from a specific matched pair. In this section H will be a finite Hopf algebra in C and we will denote by $\widehat{H} := (H^{cop})^*$, the dual of the coopposite Hopf algebra of H.

Lemma 5. *The 4-tuple $(\widehat{H}, H, \varphi_{\widehat{H}}, \phi_H)$ is a matched pair of Hopf algebras in* C, *where*

$$\varphi_{\widehat{H}} := (H^* \otimes b_H(K)) \circ (H^* \otimes R \otimes H^*) \circ (a_H(K) \otimes H \otimes H^*),$$
$$\phi_H := (H \otimes b_H(K)) \circ (\overline{R} \otimes H^*),$$

and R and $\overline{R}$ are defined as follows:

$$R := \mu_H \circ c_{H,H} \circ (\mu_H \otimes \lambda_H^{-1}) \circ (H \otimes \delta_H),$$
$$\overline{R} := (H \otimes (\mu_H \circ (\lambda_H^{-1} \otimes H))) \circ (\delta_H \otimes H) \circ c_{H,H} \circ \delta_H.$$

Moreover, the bicrossed product Hopf algebra of $\widehat{H}$ with H obtained from the previous matched pair coincides with the Drinfeld Double of H, i.e., $D(H) = \widehat{H} \bowtie H$.

Thus, particularizing Theorem 3 to the previous situation, the following is obtained:

Theorem 6. *If H is a cocommutative Hopf algebra, then $(\widehat{H} \otimes H, D(H))$ is a Hopf brace.*

On the other hand, the following result is obtained as a corollary of Theorem 4 particularized to the situation presented in Lemma 5:

Theorem 7. *If H is a commutative Hopf algebra, then $(D(H), \widehat{H} \otimes H)$ is a Hopf brace.*

All proofs in this presentation were carried out using the *tapestry technique* [4], which enables 2-dimensional graphical calculus in (braided) monoidal categories. The audience is challenged to develop a program that automatically generates these diagrams.

Acknowledgements. Both authors have been partially supported by Ministerio de Ciencia e Innovación. Agencia Estatal de Investigación (grant no. PID2020-115155GB-I00 and PID2024-155502NB-I00). The second author has been partially supported by Xunta de Galicia through the Competitive Reference Groups (grant no. ED431C 2023/31) and through a PhD fellowship (grant no. ED481A-2023-023).

References

[1] I. Angiono, C. Galindo, L. Vendramin: Hopf braces and Yang-Baxter operators. *Proc. Am. Math. Soc.* **145**(5), 1981–1995 (2017).

[2] Y. Doi, M. Takeuchi: Multiplication alteration by two-cocycles - the quantum version. *Comm. Algebra* **22**(14), 5715–5732 (1994).

[3] R. González Rodríguez: The fundamental theorem of Hopf modules for Hopf braces. *Linear Multilinear Algebra* **70**(20), 5146–5156 (2022).

[4] R. González Rodríguez: Distributive laws in non associative setting. To appear in *Functor and Tensor Categories, Models, and Systems*, Springer Proceedings in Mathematics & Statistics (2026).

[5] R. González Rodríguez, B. Ramos Pérez: About Hopf braces and crossed products. To appear in *São Paulo J. Math. Sci.* (2026).

[6] L. Guarnieri, L. Vendramin: Skew braces and the Yang–Baxter equation. *Math. Comput.* **86**(307), 2519–2534 (2017).

[7] S. Majid: *Foundations of quantum group theory*. Cambridge University Press, Cambridge (1995).

[8] W. Rump: Braces, radical rings, and the quantum Yang–Baxter equation. *J. Algebra* **307**(1), 153–170 (2007).

On the eigenvalues of QM-matrices and $Q^{1,2}$-matrices

L. González-Vega
CUNEF Universidad
laureano.gonzalez@cunef.edu

Abstract. Q-matrices are matrices whose sums of principal minors of the same order are positive. A matrix is a QM-matrix if all its powers are Q-matrices. We will characterise, up-to size 5, the real QM-matrices and those real matrices A, up-to size 4, such that A and A^2 are Q-matrices but not all eigenvalues of A have positive real part.

This is work accepted for publication at ICLR'26 [1].

Introduction

P-matrices are matrices all of whose principal minors are positive. Q-matrices are matrices whose sums of principal minors of the same order are positive. A matrix is a PM-matrix if all its powers are P-matrices. A matrix is a QM-matrix if all its powers are Q-matrices. The study of the eigenvalues of these matrices brings many open questions. For example, until 2024 (see [5]), it was not known if the eigenvalues of a PM-matrix were necessarily positive (solving a longstanding conjecture raised in [4]). Or it is not known if the eigenvalues of a matrix A such that A and A^2 are P-matrices necessarily have positive real parts (see [3]). Taking into account that a P (resp. PM) matrix is a Q (resp. QM) matrix, we will study these questions for Q-matrices and QM-matrices in order to find an answer for the original problems. In this paper, by using Symbolic Computation, we will characterise the real QM-matrices up-to size 5 and we characterise those real matrices A, 4×4, such that A and A^2 are Q-matrices but not all eigenvalues of A have positive real part.

Two ingredients will be used in order to approach these two questions symbolically. The first one is Descartes Rule of Signs (see [1, 2]) allowing us to conclude that if $\lambda \in \mathbb{R}$ is an eigenvalue of a Q-matrix or a QM-matrix or a P-matrix or a PM-matrix then $\lambda > 0$. The second one will allow us to compute easily the characteristic polynomial of A^n: if $C_A(T)$ is the characteristic polynomial of A then the characteristic polynomial of A^n agrees with the resultant of $C_A(Y)$ and $Y^n - T$ with respect to Y.

About the eigenvalues of QM-matrices ($n \leq 5$)

In order to consider the question (introduced in [4] and solved in [5]) asking if the eigenvalues of a PM-matrix are positive real numbers we analyse the same question for QM-matrices. If the eigenvalues of any QM-matrix are positive real numbers then the eigenval-

J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, V. Sotomayor (eds.): Proceedings of the XIX EACA, pp. 151-156 (2026).
ISBN: 978-84-09-87277-0

ues of any PM-matrix will be positive too. In this section we prove that this happens when $n \leq 4$ but not for $n = 5$.

The analysis performed will use the following fact (see [4]): if λ is an eigenvalue of a QM-matrix A then $|\lambda|$ is also an eigenvalue of A. This automatically implies that if A is a QM-matrix of size 2 over $\mathbb{R}$ then (because Descartes Rule of Signs) their eigenvalues are positive real numbers (they can not be complex and non-real numbers: in that case their modulus will be an eigenvalue of A).

Eigenvalues of a QM-matrix when $n = 3$

Let A be a QM-matrix of size 3 over $\mathbb{R}$. Regarding the three eigenvalues of A, we have only two possibilities:

1. The three eigenvalues of A are positive real numbers (Descartes Rule of Signs).
2. One of them is real, λ, and two complex non-real, $\lambda(\cos(\alpha) \pm i\sin(\alpha))$, $\alpha \neq 0$: λ is positive according to Descartes Rule of Signs.

In the second case, since the characteristic polynomial of A^n is

$$C_{A^n}(T) = T^3 - \lambda^n (1 + 2\cos(n\alpha)) T^2 + \lambda^{2n} (2\cos(n\alpha) + 1) T - \lambda^{3n}$$

we have, for all n, $2\cos(n\alpha) > -1$. Then $\alpha \in \bigcap_{n=1}^{\infty} \left(-\frac{2\pi}{3n}, \frac{2\pi}{3n}\right) = \{0\}$, which is not possible.

Eigenvalues of a QM-matrix when $n = 4$

Let A be a QM-matrix of size 4 over $\mathbb{R}$. Regarding the four eigenvalues of A, we have two possibilities (the case of having 4 non real eigenvalues is excluded since this implies their modules to be also eigenvalues of A):

1. The four eigenvalues of A are positive real numbers (Descartes Rule of Signs).
2. Two of them are real, λ_1 and λ_2, and two non-real, $\rho(\cos(\alpha) \pm i\sin(\alpha))$ ($\alpha \neq 0$): $\lambda_1 > 0$, $\lambda_2 > 0$ (according to Descartes Rule of Signs) and $\lambda_1 = \rho$ or $\lambda_2 = \rho$.

In the second case, after computing $C_{A^n}(T)$, we have that, for all n, $2\cos(n\alpha) > -\frac{1+L_1^n L_2^n}{L_1^n + L_2^n}$ where $L_i = \frac{\lambda_i}{\rho}$ (i.e. $L_1 = 1$ or $L_2 = 1$). Like before, this implies $\alpha = 0$, which is not possible.

Eigenvalues of a QM-matrix when $n = 5$

Let A be a QM-matrix of size 5 over $\mathbb{R}$. Regarding the five eigenvalues of A, we have three possibilities:

1. The five eigenvalues of A are positive real numbers (Descartes Rule of Signs).
2. $\rho > 0$, $\rho(\cos(\alpha) \pm i\sin(\alpha))$ and $\rho(\cos(\beta) \pm i\sin(\beta))$ with $\alpha\beta \neq 0$.

3. $\rho > 0$, $\rho(\cos(\alpha) \pm i \sin(\alpha))$ ($\alpha \neq 0$), $\lambda > 0$ and $\tau > 0$.

In the second case, after determining $C_{A^n}(T)$, we conclude that A is a QM-matrix iff $1 + 2\cos(n\alpha) + 2\cos(n\beta) > 0$ and $1 + 2\cos(n\alpha)\cos(n\beta) + \cos(n\beta) + \cos(n\alpha) > 0$ for all n. But this implies $\alpha = 0$ or $\beta = 0$, which is not possible. Figure 1 shows those (α, β) veryfying the two previous inequalities when $n \leq 8$.

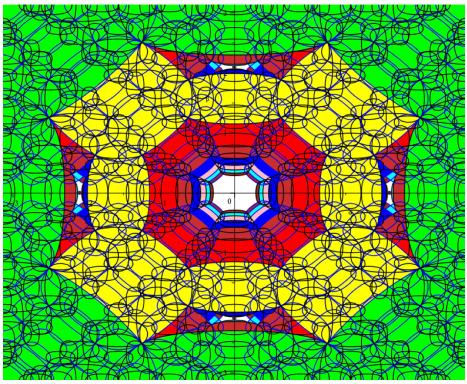


Figure 1. Solution (white) of $1 + 2\cos(n\alpha) + 2\cos(n\beta) > 0$ *and* $1 + 2\cos(n\alpha)\cos(n\beta) + \cos(n\beta) + \cos(n\alpha) > 0$, *for all* $n \leq 8$.

In the third case, if $L_1 = \frac{\lambda}{\rho}$, $L_2 = \frac{\tau}{\rho}$ and $L = \min\{L_1, L_2\}$ then, after determining $C_{A^n}(T)$, we conclude $\cos(n\alpha) > -\frac{1}{2} - \frac{1}{2}\frac{1}{L^n}$ for all n. But this implies $\alpha = 0$ or $\alpha = \pm\frac{2\pi}{3}$ (this computation is quite involved and requires to use `Maple` in a non trivial way). This implies that the eigenvalues of a QM-matrix ($n \geq 5$) are not necessarily positive real numbers while the situation for PM-matrices is different (see [5]): their eigenvalues are always positive.

About the eigenvalues of $Q^{1,2}$-matrices ($n \leq 4$)

A square matrix A is a $Q^{1,2}$-matrix if A and A^2 are Q-matrices. We shall characterize the eigenvalues of these matrices in order to know when these conditions imply (or not) the considered matrix to be positive stable (i.e. when all its eigenvalues have positive real part). There is an open problem asking if A and A^2 are P-matrices then A is positive stable (see [3]) and the obtained characterization here provides candidates where to find counterexamples to this conjecture (in case they exist).

A different approach to the one considered in [3] is introduced here for proving that for $n = 4$ there exists $Q^{1,2}$-matrices not being positive stable.

Eigenvalues of a $Q^{1,2}$-matrix when $n = 2$

Let A be a $Q^{1,2}$-matrix of size 2 over $\mathbb{R}$. Regarding the two eigenvalues of A, λ_1, λ_2, we have two possibilities:

1. $\lambda_1 \in \mathbb{R}$ and $\lambda_2 \in \mathbb{R}$: both positive (Descartes Rule of Signs).
2. $\lambda_1 = \lambda \in \mathbb{C} - \mathbb{R}$ and $\lambda_2 = \overline{\lambda}$.

In the first case, A is positive stable. Next we describe, in the other case, when the eigenvalues correspond to a $Q^{1,2}$-matrix and when the corresponding matrix is (or is not) positive stable. In this case, if $\lambda = \rho\,(\cos(\alpha) + i\sin(\alpha))$ ($\alpha \neq 0$) then $C_A(T) = T^2 - 2\rho\cos(\alpha)T + \rho^2$ and $C_{A^2}(T) = T^2 - 2\rho^2\left(2\cos^2(\alpha) - 1\right)T + \rho^4$. Therefore, λ and $\overline{\lambda}$ are the eigenvalues of a $Q^{1,2}$-matrix if and only if $\cos(\alpha) > 0$ and $\cos^2(\alpha) > -1/2$. This implies that, in this particular case, A is a $Q^{1,2}$-matrix if and only if $\alpha \in (-\pi/4, \pi/4) - \{0\}$. Then, any $Q^{1,2}$-matrix of size 2 is positive stable and the conjecture in [3], regarding $P^{1,2}$-matrices of size 2, is true (when $\alpha \in (-\pi/4, \pi/4)$, we have $\cos(\alpha) > 0$).

Eigenvalues of a $Q^{1,2}$-matrix when $n = 3$ ($n \leq 4$)

Let A be a $Q^{1,2}$-matrix of size 3 over $\mathbb{R}$. Regarding the three eigenvalues of A, λ_i, we have two possibilities:

1. $\lambda_1 \in \mathbb{R}$, $\lambda_2 \in \mathbb{R}$ and $\lambda_3 \in \mathbb{R}$: all of them positive (Descartes Rule of Signs).
2. $\lambda_1 \in \mathbb{R}$, $\lambda_2 = \rho\,(\cos(\alpha) + i\sin(\alpha)) \in \mathbb{C} - \mathbb{R}$ and $\lambda_3 = \overline{\lambda}_2$: λ_1 is positive (Descartes Rule of Signs).

By using again $C_A(T)$ and $C_{A^2}(T)$ we get that A is a $Q^{1,2}$-matrix iff $0 < \frac{\sqrt{\rho^2 + 2\lambda_1^2}}{2\lambda_1} < \cos(\alpha) < 1$. We conclude that any $Q^{1,2}$-matrix of size 3 is positive stable (since $\cos(\alpha) > 0$) and the conjecture in [3], regarding $P^{1,2}$ matrices of size 3, is true.

Eigenvalues of a $Q^{1,2}$-matrix when $n = 4$

Let A be a $Q^{1,2}$-matrix of size 4 over $\mathbb{R}$. Regarding the four eigenvalues of A, λ_i, we have three possibilities:

1. $\lambda_i \in \mathbb{R}$, $1 \leq i \leq 4$: all of them positive (Descartes Rule of Signs).
2. $\lambda_1, \lambda_2 \in \mathbb{R}$, $\lambda_3 \in \mathbb{C} - \mathbb{R}$ and $\lambda_4 = \overline{\lambda}_3$: $\lambda_1 > 0$ and $\lambda_2 > 0$ (Descartes Rule of Signs).
3. $\lambda_1 \in \mathbb{C} - \mathbb{R}$, $\lambda_2 \in \mathbb{C} - \mathbb{R}$, $\lambda_3 = \overline{\lambda}_1$, and $\lambda_4 = \overline{\lambda}_2$.

If the four eigenvalues of A are real numbers then A is positive stable. Next we describe, in the remaining two cases, when the eigenvalues correspond to a $Q^{1,2}$-matrix and when the corresponding matrix is (or is not) positive stable.

In the second case, let $L_1 = \lambda_1/\rho$, $L_2 = \lambda_2/\rho$ and $Z = \cos(\alpha)$. Figure 2 shows (orange coloured) the values of L_1 and L_2 producing $Q^{1,2}$-matrices for $Z = -3/5$, $Z = -\sqrt{3}/3$, $-\sqrt{3}/3 + 0.01$, $-15/29$, $-1/2$,-0.48, $-\sqrt{18 - 6\sqrt{3}}/6$, $-1/3$, 0, $1/3$, $\sqrt{18 - 6\sqrt{3}}/6$, $1/2 - 0.01$, $1/2$, $\sqrt{2}/2 - 0.1$ and $\sqrt{2}/2$ (from left to right). This implies, for example, that if $\cos(\alpha) \in \left(-1, -\frac{\sqrt{3}}{3}\right] \cup \left[-\frac{\sqrt{18-6\sqrt{3}}}{6}, \frac{\sqrt{18-6\sqrt{3}}}{6}\right]$ then there are no $Q^{1,2}$-matrices with λ_1, λ_2, λ and $\overline{\lambda}$ as eigenvalues.

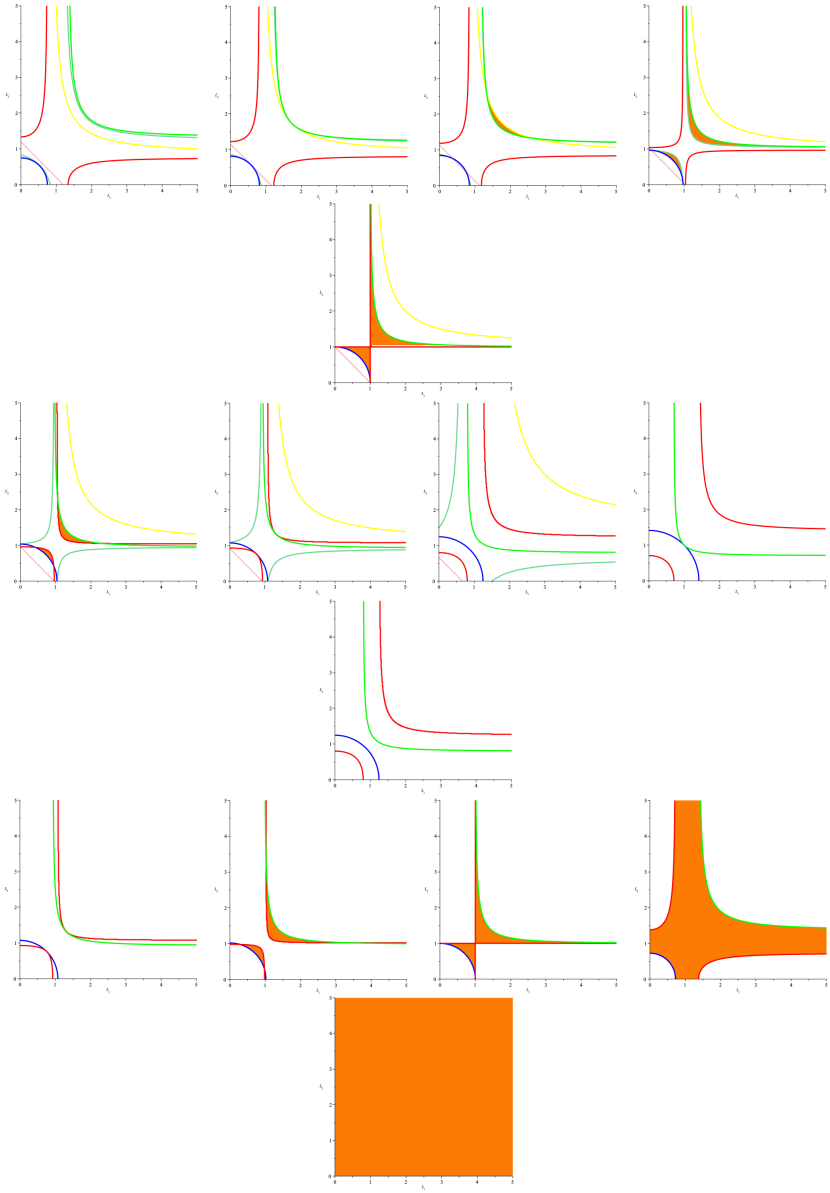


Figure 2

The matrix

$$\begin{pmatrix} 19 & 0 & 0 & 0 \\ 0 & 16 & 0 & 0 \\ 0 & 0 & -\frac{180}{29} & -\frac{24\sqrt{154}}{29} \\ 0 & 0 & \frac{24\sqrt{154}}{29} & -\frac{180}{29} \end{pmatrix}$$

is one concrete example of a $Q^{1,2}$-matrix not positive stable.

In the third case, if ω and ρ are the modulus of the eigenvalues of A then, by using again $C_A(T)$ and $C_{A^2}(T)$, A is a $Q^{1,2}$-matrix not positive stable iff $\frac{1}{\sqrt{3}} < \frac{\omega}{\rho} < \sqrt{3}$.

Conclusions

Symbolic Computation was used to generate $C_{A^k}(T)$ (by using resultants) and simplifying the trigonometric expressions appearing as coefficients. The complicated systems of inequalities involved were solved by initially treating them with `Maple`. The obtained results are a first step towards the characterization of the eigenvalues of QM-matrices and $Q^{1,2}$-matrices.

References

[1] S. Basu, R. Pollack, M.F. Roy: *Algorithms in real algebraic geometry*. Algorithms and computations in mathematics **10**, Springer-Verlag (2003).

[2] L. Gonzalez-Vega, J.R. Sendra, J. Sendra: Eigenvalues of real matrices with prescribed principal minors sign and Descartes law of signs. *ArXiv:2305.08861* (2023).

[3] D. Hershkowitz, N. Keller: Positivity of principal minors, sign symmetry and stability. *Linear Algebra Appl.* **364**, 105–124 (2003).

[4] D. Hershkowitz, C.R. Johnson: Spectra of matrices with P-matrix powers. *Linear Algebra Appl.* **80**, 159–171 (1986).

[5] S. Mondal, K.C. Sivakumar, M.J. Tsatsomeros: P-matrix powers. *Linear Algebra Appl.* **699**, 355–366 (2024).

On the annihilator and Bernstein-Sato polynomial of a rational function

M. González-Villa*, E. León-Cardenal◇*, V. Levandovskyy†, J. Martín-Morales*

◇ *Speaker at EACA 2026*

* *Departamento de Matemáticas, IUMA, Universidad de Zaragoza*

† *EPAM School of Digital Technologies, American University Kyiv*

m.gonzalez@unizar.es, eleon@unizar.es, viktor.levandovskyy@auk.edu.ua, jorge.martin@unizar.es

Abstract. We present an algorithmic approach for computing the recently introduced Bernstein-Sato polynomial of a rational function. In order to compute the annihilator of the rational function we use the annihilator of the pair consisting of the numerator and denominator of the quotient. A non-vanishing condition on the Bernstein-Sato ideal of the pair pops up in a natural way giving the annihilator of the quotient as the saturation of the annihilator of the pair. The method has been implemented in Singular and relies on Gröbner bases in noncommutative PBW algebras. Our algorithm allows us to exhibit, for the first time, some explicit non-trivial examples of Bernstein-Sato polynomials of rational functions.

Introduction

A classic problem in singularity theory is the understanding of the singularities of meromorphic functions. Finding good invariants of such functions or extending the definition of known invariants to the meromorphic case is often a challenging problem. Given two polynomials f, g in $\mathbb{C}[x] := \mathbb{C}[x_1, \ldots, x_n]$, we study in this paper the recently introduced Bernstein-Sato polynomial of the rational function $\frac{f}{g}$. Let D be the nth Weyl algebra over $\mathbb{C}$, and consider the algebra $D[s] = D \otimes_{\mathbb{C}} \mathbb{C}[s]$, where s is another variable. By $\mathbb{C}[x, s, \frac{1}{fg}]$ we denote the localization of $\mathbb{C}[x, s]$ with respect to the multiplicatively closed set $\{(fg)^k\}_{k \in \mathbb{Z}_{\geq 0}}$. Following Takeuchi [10], the Bernstein-Sato polynomial of $\frac{f}{g}$, related to a given nonnegative integer m, is the monic polynomial of smallest degree satisfying the relation

$$b_{\frac{f}{g},m}(s) \frac{1}{g^m} \left(\frac{f}{g}\right)^s \in \sum_{k=1}^{\infty} D[s] \frac{1}{g^m} \left(\frac{f}{g}\right)^{s+k}, \tag{1}$$

in the free $\mathbb{C}[x, s, \frac{1}{fg}]$-module of rank one $\mathbb{C}[x, s, \frac{1}{fg}] \left(\frac{f}{g}\right)^s$, see [1] for a similar construction. The polynomial $b_{\frac{f}{g},m}(s)$ is shown to satisfy some expected relations with respect to other invariants of the singularity of rational functions. However, only trivial examples are known.

J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, V. Sotomayor (eds.): Proceedings of the XIX EACA, pp. 157-160 (2026).
ISBN: 978-84-09-87277-0

Annihilator of a rational function

Given two non-constant polynomials $f, g \in \mathbb{C}[x_1, \ldots, x_n]$, Sabbah [9] showed the existence of a nonzero polynomial $b(s_1, s_2) \in \mathbb{C}[s_1, s_2]$ such that $b(s_1, s_2) f^{s_1} g^{s_2} = P(s_1, s_2) f^{s_1+1} g^{s_2+1}$, where $P(s_1, s_2) \in D[s_1, s_2] = D \otimes_{\mathbb{C}} \mathbb{C}[s_1, s_2]$. The set of polynomials satisfying this functional equation forms an ideal in $\mathbb{C}[s_1, s_2]$, which is called the *Bernstein-Sato ideal* of f, g, and is denoted by $B_{f,g}$. On the other hand, it is not difficult to show that the free $\mathbb{C}[x, s, \frac{1}{fg}]$-module of rank one $\mathbb{C}\left[x, s, \frac{1}{fg}\right]\left(\frac{f}{g}\right)^s$, has a natural structure of $D[s]$-module. This is the place where Takeuchi's construction for the Bernstein-Sato polynomial of $\frac{f}{g}$ takes place.

Theorem 1. ([10, Theorem 1.1]) *Given a nonnegative integer m there exists a nonzero polynomial $b_{\frac{f}{g},m}(s) \in \mathbb{C}[s]$, verifying* (1).

One reason to use the parameter m in the definition of $b_{\frac{f}{g},m}(s)$ is its relation to the local Milnor monodromy of the rational function $\frac{f}{g}$. Following Oaku's original ideas [8], we compute the annihilator in $D[s]$ of $\frac{1}{g^m}\left(\frac{f}{g}\right)^s$, denoted by, $I_m(s) := \mathrm{Ann}_{D[s]} \frac{1}{g^m}\left(\frac{f}{g}\right)^s$. Towards this computation, we first compute the annihilator in $D[s_1, s_2]$ of $f^{s_1} g^{s_2}$, denoted by $I(s_1, s_2)$. After the substitution $s_1 = s$ and $s_2 = -s-m$ we obtain a new ideal $I(s, -s-m)$ in $D[s]$ that it is in general not $\mathbb{C}[s]$-saturated. Hence $I(s, -s-m) \neq I_m(s)$. Our first main result is a sufficient condition for the saturation of $I(s, -s-m)$ to be equal to $I_m(s)$.

Definition 2. We say that $b(s_1, s_2) \in B_{f,g}$ satisfies the $\mathcal{C}_m$-*condition* if $b(s-i, -s-m-i) \neq 0$, for all $i \in \mathbb{Z}$, $i \geq 1$. Moreover we say that the ideal $B_{f,g}$ satisfies the $\mathcal{C}_m$-*condition* if there exists $b(s_1, s_2) \in B_{f,g}$ satisfying the $\mathcal{C}_m$-condition.

Note that the previous $\mathcal{C}_m$-condition can be established algorithmically, once the Bernstein ideal has been computed. Recall that given a left ideal $I \subset D[s]$, the $\mathbb{C}[s]$-*saturation* of I is the left ideal

$$\mathrm{Sat}_{\mathbb{C}[s]}(I) := \{P(s) \in D[s] \mid \exists q(s) \in \mathbb{C}[s] \setminus \{0\},\ q(s)P(s) \in I\}.$$

This ideal contains I and we say that I is $\mathbb{C}[s]$-*saturated* if the equality $I = \mathrm{Sat}_{\mathbb{C}[s]}(I)$ holds. Analogously, we define this notion for a left ideal $I \subset D[s_1, \ldots, s_\ell]$ for $\ell \geq 2$. The $\mathbb{C}[s]$-saturation of $I \subset D[s]$ can be computed by using the algorithms in [3, 5].

Theorem 3. ([4, Theorem 4.5]) *Assume that the Bernstein-Sato ideal $B_{f,g}$ satisfies the $\mathcal{C}_m$-condition. Then $I_m(s) = \mathrm{Sat}_{\mathbb{C}[s]}(I(s, -s-m))$.*

If $B_{f,g}$ does not satisfy the $\mathcal{C}_m$-condition, we compute $I_m(s)$ by following an alternative approach based on Lemma 4. Take a fixed $P(s) \in D[s]$ and let $\{Q_1(s), \ldots, Q_r(s)\} \subset D[s]$ be a system of generators of a left ideal $I \subset D[s]$. Consider $\pi : D[s]^{r+1} \to D[s]$ the canonical projection onto the first factor. By abuse of notation we denote by $\mathrm{syz}_{D[s]}(P(s), I)$ the left submodule $\mathrm{syz}_{D[s]}(P(s), Q_1(s), \ldots, Q_r(s)) \subset D[s]^{r+1}$.

Lemma 4. ([4, Lemma 4.9]) *Equality $I_{k-i}(s) = \pi\left(\mathrm{syz}_{D[s]}\left(f^i, I_k(s-i)\right)\right)$, holds $\forall i \geq 0$.*

Bernstein-Sato polynomial of rational functions

Let $f, g \in \mathbb{C}[x_1, \ldots, x_n]$ be two polynomials and $m \in \mathbb{Z}$, $m \geq 0$. It follows from Theorem 1 that for a big enough N there exists a nonzero polynomial $b(s) \in \mathbb{C}[s]$ and $P_1(s), \ldots, P_N(s) \in D[s]$ such that $b(s)\frac{1}{g^m}\left(\frac{f}{g}\right)^s = \sum_{k=1}^{N} P_k(s)\frac{1}{g^m}\left(\frac{f}{g}\right)^{s+k}$. The set of polynomials $b(s)$ verifying this functional equation is an ideal, and we denote by $b^{(N)}_{\frac{f}{g},m}(s)$ its monic generator. Note that, in general, given f, g, m, no upper bound for $N \geq 1$ exists, see Example 5. However, in some cases we are able to compute precisely the Bernstein-Sato polynomial as in Example 6. The equality

$$\pi\left(\mathrm{syz}_{D[s]}\left(g^N, I_{m+N}(s) + \sum_{k=1}^{N} D[s]f^k g^{N-k}\right)\right) \cap \mathbb{C}[s] = \left\langle b^{(N)}_{\frac{f}{g},m}(s)\right\rangle,$$

provides a method for computing the Bernstein-Sato polynomial of $\frac{f}{g}$, once a system of generators of $I_{m+N}(s) \subset D[s]$ has been obtained, see Algorithm 1:

Algorithm 2: Bernstein-Sato (computes $b^{(N)}_{\frac{f}{g},m}(s)$ assuming it is not zero)

Input : f, g two polynomials in $\mathbb{C}[x_1, \ldots, x_n]$; $m \geq 0$ and $N \geq 1$ integers; $<$ a monomial order on $D[s]$.
Output: $b^{(N)}_{\frac{f}{g},m}(s) \in \mathbb{C}[s]$.

begin
  $I := I_{m+N}(s)$, $J := I + D[s]\langle fg^{N-1}, f^2g^{N-2}, \ldots, f^N\rangle$, $G :=$ Gröbner basis of J with respect to $<$;
  $P_0 := NF(g^N, G)$;
  if $P_0 = 0$ **then**
    return $b = 1$;
  end
  $k := 1$;
  while *true* **do**
    $P_k = NF(s^k g^N, G)$;
    if $\exists a_0, \ldots, a_k \in \mathbb{Q}$ *(with* $a_k = 1$*) such that* $a_0P_0 + \ldots + a_kP_k = 0$ **then**
      return $b = a_0 + a_1 s + \ldots + a_k s^k$;
    end
    $k := k + 1$;
  end
end

Examples

Example 5. Consider $f = x^2 + y^3$ and $g = xy$. For all $m \geq 0$ the ideal $I(s, -s - m)$ is $\mathbb{C}[s]$-saturated and the Bernstein-Sato ideal satisfies the $\mathcal{C}_m$-conditions. Running Algorithm 1 for $m = 0$ one obtains $b^{(1)}_{\frac{f}{g},0}(s) = (s+1)(s+5)(s+7), b^{(N)}_{\frac{f}{g},0}(s) = (s+1)(s+5)$, for $N = 2, \ldots, 5$, and $b^{(6)}_{\frac{f}{g},0}(s) = s + 1 = b^{(N)}_{\frac{f}{g},0}(s)$ for all $N \geq 6$. On the other hand, for $m = 1$, Algorithm 1 yields $b^{(1)}_{\frac{f}{g},1}(s) = s(s+1)(s+2)$, and $b^{(N)}_{\frac{f}{g},1}(s) = s(s+1)$ for $N = 2, \ldots, 20$. However, we could not verify whether $b^{(N)}_{\frac{f}{g},1}(s) = s + 1$ for N big enough as in case $m = 0$.

Example 6. Let $f = x^2 + y^3$, $g = x$, and $m = 4$. The Bernstein-Sato ideal satisfies the $\mathcal{C}_m$-condition and the ideal $I(s, -s - m)$ is $\mathbb{C}[s]$-saturated for all $m \geq 0$. Algorithm 1 for $N = 1$

produces $b^{(1)}_{\frac{f}{g},4}(s) = \left(s+1\right)\left(s-\frac{7}{3}\right)\left(s-\frac{5}{3}\right)$. Studying the eigenvalues of the monodromy of the rational function f/g. We can show that in fact $b^{(1)}_{\frac{f}{g},4}(s) = b^{(N)}_{\frac{f}{g},4}(s)$ for every $N \geq 1$.

Example 7. Consider $f = x^6 + y^6 + 2zx^3y^3$ and $g = z^2$. Then $B_{f,g}$ satisfies the $\mathcal{C}_m$-condition for all $m \geq 0$. Furthermore, the ideal $I(s, -s-m)$ is $\mathbb{C}[s]$-saturated for all $m \geq 2$, while $I(s, -s-1)$ is not. In fact, $I_1(s) = \mathrm{Sat}_{\mathbb{C}[s]}(I(s, -s-1)) = I(s, -s-1) : \left(s+\frac{1}{2}\right) \supsetneq I(s, -s-1)$. Algorithm 1 for $m = 0$ and $N = 1, \ldots, 4$ yields

$$b^{(N)}_{\frac{f}{g},0}(s) = \left(s+1\right)^2\left(s+\frac{1}{2}\right)\left(s+\frac{3}{2}\right)\left(s+\frac{1}{3}\right)\left(s+\frac{2}{3}\right)\left(s+\frac{4}{3}\right)\left(s+\frac{5}{6}\right)\left(s+\frac{7}{6}\right).$$

Acknowledgements. The first and second authors have been partially supported by PID2024-156181NB-C33 funded by MICIU/AEI/10.13039/501100011033 and by FEDER, UE. Also supported by SECIHTI project CF-2023-G33. The fourth author has been supported by CNS2024-154271 and RYC2021-034300-I funded by MICIU/AEI/10.13039/501100011033 and the European Union NextGenerationEU/PRTR. Also supported by Junta de Andalucía (FQM-333).

References

[1] J. Álvarez Montaner, M. González Villa, E. León-Cardenal, L. Núñez Betancourt: Bernstein-Sato polynomial and related invariants for meromorphic functions. *Trans. Amer. Math. Soc.* **378**(7), 4929–4954 (2025).

[2] D. Andres, V. Levandovskyy: *bfun.lib, A Singular 4-2-0 library for computing b-functions and Bernstein-Sato polynomials*. `http://www.singular.uni-kl.de` (2012).

[3] T. Becker, V. Weispfenning: *Gröbner bases*. Graduate Texts in Math **141**, Springer-Verlag (1993).

[4] M. González-Villa, E. León-Cardenal, V. Levandovskyy, J. Martín-Morales: An algorithm for annihilator and Bernstein-Sato polynomial of a rational function. *ArXiv:2602.00280* (2026).

[5] J. Hoffmann, V. Levandovskyy: Constructive arithmetics in Ore localizations enjoying enough commutativity. *J. Symbolic Comput.* **102**, 209–230 (2021).

[6] V. Levandovskyy, J. Martín-Morales: *dmod.lib, A Singular 4-2-0 library for algebraic D-modules*. `http://www.singular.uni-kl.de` (2010).

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

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

[9] C. Sabbah: Proximité évanescente. II. Équations fonctionnelles pour plusieurs fonctions analytiques. *Compositio Math.* **64**(2), 213–241 (1987).

[10] K. Takeuchi: On a Bernstein-Sato polynomial of a meromorphic function. *Nagoya Math. J.* **251**, 715–733 (2023).

Tensor learning with orthogonal, Lorentz, and symplectic symmetries

W.G. Gregory*, J. Tonelli-Cueto◇†, N.F. Marshall‡, A.D. Lee≀, S. Villar*

◇ *Speaker at EACA 2026*

* *Johns Hopkins University*

† *CUNEF Universidad*

‡ *Oregon State University*

≀ *Adelphi University*

wgregor4@jhu.edu, josue.tonelli.cueto@bizkaia.eu, marsnich@oregonstate.edu, alee2@adelphi.edu, svillar3@jhu.edu

Abstract. Tensors are a fundamental data structure for many scientific contexts, such as time series analysis, materials science, and physics, among many others. Improving our ability to produce and handle tensors is essential to efficiently address problems in these domains. In this talk, we show how to exploit the underlying symmetries of functions that map tensors to tensors. More concretely, we develop universally expressive equivariant machine learning architectures on tensors that exploit that, in many cases, these tensor functions are equivariant with respect to the diagonal action of the orthogonal, Lorentz, and/or symplectic groups. We showcase our results on three problems coming from material science, theoretical computer science, and time series analysis. For time series, we combine our method with the increasingly popular path signatures approach, which is also invariant with respect to reparameterizations. Our numerical experiments show that our equivariant models perform better than corresponding non-equivariant baselines.

This is work accepted for publication at ICLR'26 [1].

Introduction

Tensors are fundamental mathematical objects that appear in a broad spectrum of domains. In many problems in the sciences and engineering, we find tensor-valued data at their center. In these settings, we are interested in learning functions of the form

$$(a_1, \dots, a_n) \mapsto f(a_1, \dots, a_n)$$

that map a tuple of tensors to another tuple of tensors. Moreover, in many applications, such as physics (see [1] for references, we expect such tensor-maps to be equivariant to some group action, such as the natural action of the orthogonal group on tensors. Using these symmetries, we can reduce the number of parameters to be learned in our training model, but, more importantly, we can guarantee better generability of the learned function outside the training data.

J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, V. Sotomayor (eds.): Proceedings of the XIX EACA, pp. 161-165 (2026).
ISBN: 978-84-09-87277-0

In this communication, based on [1], we develop universally expressive equivariant machine learning architectures for equivariant tensor-maps with respect not only the natural actions of the usual orthogonal, Lorentz and symplectic groups but a wider class of real linear algebraic groups. Further, our numerical experiments showcase the advantage of our arquitectures in three cases: stress-strain tensors from material science, path signature tensors from data analysis and sparse vector estimation from computer science.

In this extended abstract, we will focus on the parameterization of equivariant tensor maps as this is the core theoretical contribution more in line with EACA. We refer to [1] for details regarding the numerical experiments.

Orthogonal Case

The orthogonal group $O(d)$ acts on vectors of $\mathbb{R}^d$ through two possible actions:

$$g \cdot v = \det(g)^{\frac{1-p}{2}} gv$$

where $p \in \{-1, 1\}$. This gives us two $O(d)$-modules: $\mathcal{T}_1(\mathbb{R}^d, -1)$ and $\mathcal{T}_1(\mathbb{R}^d, +1)$, called, respectively, *pseudovectors* and *vectors* in physics to keep track of which $O(d)$-action we are considering. This action extends naturally to tensors through the tensor product as follows:

$$\mathcal{T}_k(\mathbb{R}^d, p) := \mathcal{T}_1(\mathbb{R}^d, p_1) \otimes \cdots \otimes \mathcal{T}_1(\mathbb{R}^d, p_k)$$

where $p = p_1 \cdots p_k$. Such an $O(d)$-module depends only on p and not the particular p_i and, in physics, we call the objects in it $k_{(p)}$-*tensors*, which allows us to keep track of the kind of action.

In this setting, we are interested in parameterizing the $O(d)$-equivariant maps of the form $f : \prod_{i=1}^n \mathcal{T}_{k_i}(\mathbb{R}^d, p_i) \to \mathcal{T}_{k'}(\mathbb{R}^d, p')$, which are the maps satisfying $f(g \cdot a_1, \ldots, g \cdot a_n) = g \cdot f(a_1, \ldots, a_n)$ for all $g \in O(d)$ and $(a_1, \ldots, a_n) \in \prod_{i=1}^n \mathcal{T}_{k_i}(\mathbb{R}^d, p_i)$. To do so, we need to recall some further notions.

First, the $O(d)$-module of $k_{(p)}$-tensors, $\mathcal{T}_k(\mathbb{R}^d, p)$, admits an action by the symmetric group of order n, Σ_n, by just permuting the indices of the tensor. We denote this action by the right-action a^σ to stress the fact that this action commutes with the $O(d)$-action. Note that this action satisfies $(v_1 \otimes \cdots \otimes v_k)^\sigma = v_{\sigma^{-1}(1)} \otimes \cdots \otimes v_{\sigma^{-1}(k)}$.

Second, we have a k-*contraction map* $\iota_k : \mathcal{T}_{2k+k'}(\mathbb{R}^d, p) \to \mathcal{T}_{k'}(\mathbb{R}^d, p)$ that contracts together the first $2k$ indices of the tensor using the usual inner product. This map is determined by the identity

$$\iota_k(u_1 \otimes \cdots \otimes u_k \otimes v_1 \otimes \cdots \otimes v_k \otimes w_1 \otimes \cdots \otimes w_{k'}) = \langle u_1, v_1 \rangle \cdots \langle u_k, v_k \rangle \, w_1 \otimes \cdots \otimes w_{k'}$$

where $\langle \cdot, \cdot \rangle$ is the bilinear form preserved by $O(d)$ in $\mathbb{R}^d$, i.e., the usual inner product.

Third, an *isotropic* $k_{(p)}$-tensor is just a tensor in $\mathcal{T}_k(\mathbb{R}^d, p)$ that is fixed under the $O(d)$-action. In this setting, we have two special isotropic $k_{(p)}$-tensors. On the one hand, we have the *Kronecker delta*, δ, which is the isotropic $2_{(+1)}$-tensor given by $\delta_{i,j} = 1$ whenever $i = j$ and $\delta_{i,j} = 0$ otherwise. On the other hand, the *Levi-Civita symbol*, ϵ, which is

the isotropic $d_{(-1)}$-tensor given by $\epsilon_{i_1,\dots,i_d} = 1$ if $(i_1,\dots,i_d)$ is an even permutation of $(1,\dots,d)$, $\epsilon_{i_1,\dots,i_d} = -1$ if it is an odd one, and $\epsilon_{i_1,\dots,i_d} = 0$ otherwise.

We can now state the main results regarding $O(d)$-equivariant functions we prove in [1].

Theorem 1. ([1, Theorem 1]) *Let $f : \prod_{i=1}^n \mathcal{T}_{k_i}(\mathbb{R}^d, p_i) \to \mathcal{T}_{k'}(\mathbb{R}^d, p')$ be an $O(d)$-equivariant polynomial function of degree at most R. Then we may write f as follows:*

$$f(a_1,\dots,a_n) = \sum_{r=0}^{R} \sum_{1\le \ell_1 \le \dots \le \ell_r \le n} \iota_{k_{\ell_1,\dots,\ell_r}}(a_{\ell_1} \otimes \dots \otimes a_{\ell_r} \otimes c_{\ell_1,\dots,\ell_r})$$

where $c_{\ell_1,\dots,\ell_r}$ is an $O(d)$-isotropic $(k_{\ell_1,\dots,\ell_r} + k')_{(p_{\ell_1,\dots,\ell_r} p')}$-tensor with order and parity chosen to be consistent with the output's ($k_{\ell_1,\dots,\ell_r} = \sum_{q=1}^r k_{\ell_q}$ and $p_{\ell_1,\dots,\ell_r} = \prod_{q=1}^r p_{\ell_q}$).

The above theorem gives an effective parameterization, because we can parameterize the $O(d)$-isotropic $k_{(p)}$-tensors using the Kronecker delta and Levi-Civita symbol. See [1, Appendix C] and references therein for more details.

Lemma 2 (Characterization of $O(d)$-isotropic $k_{(p)}$-tensors)**.** *Suppose $c \in \mathcal{T}_k(\mathbb{R}^d, p)$ is $O(d)$-isotropic. Then the following holds:*

Case $p = +1$*: Assume $p = +1$. If k is even, then c can be written in the form $c = \sum_{\sigma\in\Sigma_k} \alpha_\sigma (\delta^{\otimes \frac{k}{2}})^\sigma$ where $\alpha_\sigma \in \mathbb{R}$. Otherwise, if k is odd, then $c = 0$ is the zero tensor.*

Case $p = -1$*: Assume $p = -1$. If $k - d$ is even and $k \ge d$, then c can be written in the form $c = \sum_{\sigma\in S_k} \beta_\sigma (\delta^{\otimes \frac{k-d}{2}} \otimes \epsilon)^\sigma$ where $\beta_\sigma \in \mathbb{R}$. Otherwise, if $k - d$ is odd or $k < d$, then $c = 0$ is the zero tensor.*

We note that not all permutations are needed in the above expressions, we refer to [1, Appendix D] for further details. In the following special case, we get a simpler form:

Corollary 3. ([1, Corollary 1]) *Let $f : \prod_{i=1}^n \mathcal{T}_1(\mathbb{R}^d, +) \to \mathcal{T}_{k'}(\mathbb{R}^d, +)$ be an $O(d)$-equivariant polynomial function. Then, we may write it as*

$$f(v_1,\dots,v_n) = \sum_{t=0}^{\lfloor \frac{k'}{2} \rfloor} \sum_{\sigma\in S_{k'}} \sum_{1\le J_1 \le \dots \le J_{k'-2t} \le n} q_{t,\sigma,J}((\langle v_i, v_j\rangle)_{i,j=1}^n)\, (v_{J_1} \otimes \dots \otimes v_{J_{k'-2t}} \otimes \delta^{\otimes t})^\sigma,$$

where $J = (J_1,\dots,J_{k'-2t})$ are indices of the input tensors, and the function $q_{t,\sigma,J}$ which depends on the tuple (t,σ,J) is a polynomial of the inner products of the input vectors.

General Case

The above tensor setting for the orthogonal group can be generalized easily for groups beyond the orthogonal group. We refer to [1, Section 4 and Appendix G] for the proofs and all the details. Now, consider a self-paired real vector space $(V, \langle\cdot,\cdot\rangle)$, where $\langle\cdot,\cdot\rangle$ is a non-degenerate (not necessarily symmetric) bilinear form. Through the tensor product and its universal property we get too self-paired real vector spaces of tensors $(V^{\otimes k}, \langle\cdot,\cdot\rangle)$. Now, if we have a group G acting (rationally) on $(V, \langle\cdot,\cdot\rangle)$ in a structure-preserving way (i.e., linearly, preserving $\langle\cdot,\cdot\rangle$), we have, through the universal property of tensor product,

an extension of this action to the $(V^{\otimes k}, \langle\cdot,\cdot\rangle)$. In this setting, we get the family of (rational) G-modules

$$\mathcal{T}_k(V,\chi) := (V^{\otimes k}, \langle\cdot,\cdot\rangle)$$

where $\chi : G \to \mathbb{R}^*$ is a one-dimensional (rational) group-homomorphism of G where the action of G satisfies $g \cdot (v_1 \otimes \cdots \otimes v_k) = \chi(g)(g \cdot v_1) \otimes \cdots \otimes (g \cdot v_k)$ for all $g \in G$ and $v_1, \ldots, v_n \in V$. In this setting, we still have G-isotropic tensors and a G-equivariant *contraction map*

$$\iota_k^G : \mathcal{T}_{2k+k'}(V,\chi) \to \mathcal{T}_{k'}(V,\chi)$$

satisfying $\iota_k^G(a \otimes b \otimes c) = \langle a, b\rangle c$ for $a, b \in \mathcal{T}_k(V,\chi_0)$, being χ_0 the trivial character, and $c \in \mathcal{T}_{k'}(V,\chi)$.

Our result then extends from orthogonal groups to the so-called class of complexly averageable real linear algebraic groups, which are not necessarily compact.

Definition 4. A real linear algebraic group G is *complexly averageable* if it's Zariski-dense in its complexification and its complexification admits a Zariski-dense compact subgroup closed under complex conjugation.

Theorem 5. *Let $G \subset GL(V)$ be either a compact or a complexly averagable real linear algebraic group acting rationally in a structure-preserving way on a self-paired vector space $(V, \langle\cdot,\cdot\rangle)$ and $f : \prod_{i=1}^n \mathcal{T}_{k_i}(V,\chi_i) \to \mathcal{T}_{k'}(V,\chi')$ a G-equivariant entire function. Then we may write f as follows:*

$$f(a_1,\ldots,a_n) = \sum_{r=0}^{\infty} \sum_{1\le \ell_1 \le \cdots \le \ell_r \le n} \iota^G_{k_{\ell_1,\ldots,\ell_r}} \left(a_{\ell_1} \otimes \ldots \otimes a_{\ell_r} \otimes c_{\ell_1,\ldots,\ell_r}\right)$$

where $c_{\ell_1,\ldots,\ell_r} \in \mathcal{T}_{k_{\ell_1,\ldots,\ell_r}+k'}(\mathbb{R}^d, \chi_{\ell_1,\ldots,\ell_r}\chi')$ is a G-isotropic tensor for $k_{\ell_1,\ldots,\ell_r} := \sum_{q=1}^r k_{\ell_q}$ and $\chi_{\ell_1,\ldots,\ell_r} = \prod_{q=1}^r \chi_{\ell_q}$.

In the special case of the *indefinite orthogonal group* (which is the linear part of the *Lorentz group* when $d = 4$ and $s \in \{1, 3\}$) and the *symplectic group*, given respectively by

$$O(s,d-s) := \{g \in \mathsf{GL}(\mathbb{R}^d) \mid g^\top \mathbb{I}_{s,d-s} g = \mathbb{I}_{s,d-s}\} \text{ and } Sp(d) := \{g \in \mathsf{GL}(\mathbb{R}^d) \mid g^\top \mathbb{J}_d g = \mathbb{J}_d\}$$

where $\mathbb{I}_{s,d-s} := \begin{pmatrix} \mathbb{I}_s & \\ & -\mathbb{I}_{d-s} \end{pmatrix}$ and $\mathbb{J}_d := \begin{pmatrix} & \mathbb{I}_{d/2} \\ -\mathbb{I}_{d/2} & \end{pmatrix}$, we get the following improvement using the permutation action. Below, $[A]_{i,j}$ denotes the 2-tensor in $(\mathbb{R}^d)^{\otimes 2}$ induced by the matrix $A \in \mathbb{R}^{d\times d}$.

Corollary 6. *Let G be either $O(s,d-s)$ or $Sp(d)$ and $f : \prod_{i=1}^n \mathcal{T}_1(\mathbb{R}^d,\chi_0) \to \mathcal{T}_k(\mathbb{R}^d,\chi_0)$, with $\chi_0(g) = 1$ for all g, be a G-equivariant entire function. Then we may write f as follows:*

$$f(v_1,\ldots,v_n) = \sum_{t=0}^{\lfloor \frac{k}{2} \rfloor} \sum_{\sigma\in S_k} \sum_{1\le J_1 \le \cdots \le J_{k-2t} \le n} q_{t,\sigma,J}(((\langle v_i, v_j\rangle_G)_{i,j=1}^n)\,(v_{J_1} \otimes \ldots \otimes v_{J_{k-2t}} \otimes \theta_G^{\otimes t})^\sigma$$

where $\langle v,w\rangle_G = v^T \mathbb{I}_{s,d-s} w$ and $\theta_G = \left[\mathbb{I}_{s,d-s}\right]_{i,j}$ if $G = O(s,d-s)$, and $\langle v,w\rangle_G = v^T \mathbb{J}_d w$ and $\theta_G = [\mathbb{J}_d]_{i,j}$ if $G = Sp(d)$, and $q_{t,\sigma,J}$ is an entire function that depends on the tuple (t,σ,J) and whose inputs are all possible inner products between the input vectors and whose output is a scalar.

References

[1] W.G. Gregory, J. Tonelli-Cueto, N.F. Marshall, A.S. Lee, S. Villar: *Tensor learning with orthogonal, Lorentz, and symplectic symmetries*. The Fourteenth International Conference on Learning Representations (2026).

Algorithmic construction of Baker-Akhiezer functions

A. Jiménez-Pastor[◇*], S.L. Rueda[*]

[◇] *Speaker at EACA 2026*

[*] *Universidad Politécnica de Madrid*

antonio.jimenezp@upm.es, sonialuisa.rueda@upm.es

Abstract. We compute eigenfunctions for commuting ordinary differential operators (ODOs). Given an operator L with non-trivial centralizer, we design a symbolic algorithm to compute the eigenfunction of all operators in the centralizer (called the Baker-Akhiezer function). In this presentation we restrict to the algebro-geometric case, where the existence of operators of coprime order is guaranteed. Our algorithm is implemented in the `dalgebra` package of SageMath.

Introduction

Let $(\mathbb{K}, \partial)$ be a differential field, whose field of constants **C** is algebraically closed and of zero characteristic. If two differential operators L and A in $\mathbb{K}[\partial]$ commute, there is a nonzero constant coefficient polynomial $f(\lambda, \mu)$ such that $f(L, A) = 0$. The curve Γ defined by $f(\lambda, \mu) = 0$ is the famous spectral curve and parametrizes the common eigenvalues of

$$L\Psi = \lambda\Psi, \qquad A\Psi = \mu\Psi.$$

The dimension of the space of common eigenfunctions Ψ is the same, for almost all points of Γ, this is the rank of the algebra $\mathbf{C}[L, A]$, the greatest common divisor of all orders [10]. Common eigenfunctions are called Baker-Akhiezer (BA) functions. They were introduced by Baker 1928 in the rank one case and then used by Akhiezer 1961 in the investigation of the spectral theory of ordinary differential operators. Later on Krichever introduced BA functions for arbitrary rank. In the rank one case, explicit formulas for BA-functions where given by Krichever, from spectral data on smooth spectral curves, and by Wilson in the case of rational unicursal spectral curves.

We present an algorithm to compute the BA-function from a ring of commuting ordinary differential operators, regardless of the kind of spectral curve it defines. For a given $L \in \mathbb{K}[\partial]$, we compute the simultaneous eigenfunction of the problem $A(y) = \theta(A)y$ for every A in the centralizer of L. In this presentation we focus on the rank 1 case, although our results will provide the greatest common right divisor of all operators $A - \theta(A)$ also in the case of higher rank. We assume that L is in normal form $L = \partial^n + u_{n-2}\partial^{n-2} + \ldots + u_1\partial + u_0$ and has a non-trivial centralizer $\mathcal{Z}(L) \neq C[L]$, equivalently the coefficients $u_{n-2}, \ldots, u_1, u_0$ satisfy a system of equations of the Gelfand-Dickey (GD) hierarchy. If $n = 2$ then u_0 is a solutions of one of the equations of the KdV hierarchy.

J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, V. Sotomayor (eds.): Proceedings of the XIX EACA, pp. 166-170 (2026).
ISBN: 978-84-09-87277-0

This algorithm requires that the field of coefficients $\mathbb{K}$ is *computable*, meaning that all operations within this field, including zero-recognition, derivation, and arithmetic operations can be automatically performed. Some examples of fields that are computable include monomial extensions, where we extend the field with a transcendental element prescribing its derivation [1], or strongly normal extensions, adding solutions of a D-algebraic equation without extending the constants [7, 8].

Results in this presentation are implemented in the open-source package `dalgebra` of SageMath [4]. This package is under active development and can be accessed from

`https://github.com/Antonio-JP/dalgebra`

In version `0.0.8`, we added a Jupyter notebook within the repository that includes computations from this presentation with the extended computations that can be seen as a showcase on how to use the software. The notebook can be accessed from

`https://github.com/Antonio-JP/dalgebra/blob/EACA-2026/notebooks/EACA26_PaperExamples.ipynb`

Centralizer for ODOs

The construction of the BA-function for a given ODO L requires it to be algebro-geometric. We define the *level of* L to be the minimal order of operators $A \in \mathcal{Z}(L) \setminus \mathbf{C}[L]$. We also define the *rank of* L as the rank of $\mathcal{Z}(L)$, the greatest common divisor of the orders of all operators in $\mathcal{Z}(L)$. Hence, L is algebro-geometric if and only if it has rank 1.

Based on the structural results from [3] and the works in [5], we know that the centralizer $\mathcal{Z}(L)$ is a $\mathbf{C}[L]$-module with finite basis $\{G_i \,:\, i \in \mathcal{O}\}$, where

1. $\mathcal{O}$ is an additive subgroup of the cyclic group $\mathbb{Z}_n$.
2. $\operatorname{ord}(G_{[m]}) \equiv m \pmod{n}$ and $\operatorname{ord}(G_{[m]})$ is minimal within the orders of those operators $A \in \mathcal{Z}(L)$ with $\operatorname{ord}(A) \equiv m \pmod{n}$.

With this rich structure, we proved in [5] that

$$\operatorname{rank}(\mathcal{Z}(L)) = n/|\mathcal{O}| = \gcd\{\operatorname{ord}(L), \operatorname{ord}(G_i) \mid i \in \mathcal{O}\}.$$

The algorithmic computation of a Goodearl's basis of $\mathcal{Z}(L)$ as a $\mathbf{C}[L]$-module was developed in [5], together with its implementation in SageMath. It relies strongly on our implementation of the GD hierarchies in [2].

Example 1. Consider the field $\mathbb{K} = \mathbf{C}\langle\wp\rangle$ for the Weierstrass $\wp$-function $\wp = \wp(x; 0, 1)$, i.e., satisfying $\wp'^2 = 4\wp^3 + 1$. Given $L = \partial^3 - 6\wp\partial - 6\wp'$, it has level 4, a $C[L]$-basis $\{1, G_1, G_2\}$ of its centralizer was computed with the algorithm in [5]

$$G_1 = -24\wp^2 - 12\wp'\partial - 8\wp\partial^2 + \partial^4, \qquad G_2 = -40\wp\wp' - 80\wp^2\partial - 20\wp'\partial^2 - 10\wp\partial^3 + \partial^5.$$

Spectral curve and Eigenfunctions

The centralizer is a commutative finitely generated C-algebra. Using a $C[L]$-basis

$$\mathcal{Z}(L) = C[L, G_i : i \in \mathcal{O}],$$

given algebraic variables λ and $\overline{\mu} = \{\mu_i : i \in \mathcal{O}\}$ we can establish a natural ring homomorphism $\phi_L : \mathbf{C}[\lambda, \overline{\mu}] \to \mathcal{Z}(L)$ defined by $\phi_L(\lambda) = L$ and $\phi_L(G_i) = \mu_i$.

Definition 2. We define a Burchnall-Chaundy (BC) ideal of L to be $\mathrm{BC}(L) = \ker(\phi_L)$.

Moreover ϕ_L establishes an isomorphism $\theta : \mathcal{Z}(L) \to C[\lambda, \overline{\mu}]/\mathrm{BC}(L)$. Furthermore, when L is algebro-geometric there is a common eigenfunction for all elements in $\mathcal{Z}(L)$ [10], i.e., there is Ψ, such that $A \cdot \Psi = \theta(A)\Psi$, for all $A \in \mathcal{Z}(L)$. This Ψ is called the *Baker-Akhiezer* (BA) function for L, that we want to formalize in the language of differential algebra and compute symbolically.

The BC ideal of L is the defining ideal of an algebraic curve $\Gamma = \mathrm{Spec}(\mathcal{Z}(L))$, the famous *spectral curve* [9]. Let $\mathbf{C}[\Gamma]$ be the coordinate ring of Γ and $\mathbb{K}[\Gamma] = \mathbb{K} \otimes \mathbf{C}[\Gamma]$, that is

$$\mathbf{C}[\Gamma] := \frac{\mathbf{C}[\lambda, \overline{\mu}]}{\mathrm{BC}(L)}, \qquad \mathbb{K}[\Gamma] := \frac{\mathbb{K}[\lambda, \overline{\mu}]}{[\mathrm{BC}(L)]},$$

where $[\mathrm{BC}(L)]$ is the differential ideal generated by $\mathrm{BC}(L)$ in $\mathbb{K}[\lambda, \overline{\mu}]$. It was shown in [6] that $\mathbb{K}[\Gamma]$ is a differential domain, with the extended derivation $\tilde{\partial}(f + [\mathrm{BC}(L)]) = \partial(f) + [\mathrm{BC}(L)]$. Hence we can consider its field of fractions $\mathbb{K}(\Gamma)$ with the natural extended derivation. We remark that $\mathbb{K}[\Gamma]$ is always constructible whenever $\mathbb{K}$ is constructible from $\mathbf{C}$.

In order to compute the BA-function, we need to compute the greatest common right divisor of $L - \lambda$ and $A - \theta(A)$ over $\mathbb{K}(\Gamma)$. Now that we have the algebraic set up, consider an element G_i in Goodearl's basis of $\mathcal{Z}(L)$, of order coprime with $\mathrm{ord}(L)$. The operators $L - \lambda$ and $G_i - \mu_i$ share a common solution Ψ if their differential resultant vanishes. This is guaranteed over $\mathbb{K}(\Gamma)$, since the differential resultant is a polynomial $f(\lambda, \mu_i)$ that belongs to $\mathrm{BC}(L)$. The first differential subresultant [9], is an order 1 differential operator $\alpha\partial + \beta$, namely the gcrd of $L - \lambda$ and $G_i - \mu_i$. In particular, it determines a unique solution Ψ that defines the BA-function for the pair $L - \lambda$ and $G_i - \mu_i$. This is the BA-function of L. It is important to remark that the choice of the operator G_i does not affect the output if we consider coefficients in $\mathbb{K}(\Gamma)$, where all relations between λ, μ_i, $i \in \mathcal{O}$ are taken into consideration in the BC ideal.

Hence, the BA-function Ψ of L is determined by $\partial(\Psi) = \phi\Psi$, where $\phi = -\beta/\alpha \in \mathbb{K}(\Gamma)$. Taking $\mathbf{C} = \mathbb{C}$ and $\partial = d/dx$, the BA-function of L is $\Psi = \exp\left(\int \phi dx\right)$. A closed-form solution for the BA-function now relies on algorithms for symbolic integration. Although difficult to solve symbolically in general, there are several cases that can be tackled easily: If $\mathbb{K}$ is a monomial extension, we can use the results in [1] to compute the solution and determine possible extensions. If the curve $\Gamma = \mathrm{Spec}(\mathcal{Z}(L))$ is rational, we can compute a rational parametrization of the curve and translate the problem into a parametric Risch's differential

equation problem [1]. Any other case will require the development of more specific algorithms for symbolic integration. Algorithm 1 summarizes the complete process to compute the closed-form of the BA-function.

Example 3 (Continuation of Example 1)**.** From the relations $G_1^2 = G_2 L, G_1 G_2 = (L^2 - 4)L$, $G_2^2 = (L^2 - 4)G_1$ we obtain a Gröbner basis of $\mathrm{BC}(L)$ as in [6],

$$\mathrm{BC}(L) = \left(\mu_1^2 - \mu_2\lambda, \quad \mu_1\mu_2 - \lambda^3 + 4\lambda, \quad \mu_2^2 - \mu_1\lambda^2 + 4\mu_1\right).$$

Thus $C[\Gamma] = \mathbf{C}[\lambda, \mu_1, \mu_2]/\,\mathrm{BC}(L)$ can be built. In addition, take $\mathbb{K}[\Gamma]$ as $\mathbf{C}[\Gamma]\langle\wp\rangle$ and $\mathbb{K}(\Gamma)$ as $\mathbf{C}(\Gamma)\langle\wp\rangle$. We compute the subresultant sequence for $L - \lambda$ and $G_1 - \mu_1$. The 0th subresultant $f(\lambda, \mu_1) = -\mu_1^3 + \lambda^4 - 4\lambda^2$ is the differential resultant of $L - \lambda$ and $G_1 - \mu_1$, which belongs to $\mathrm{BC}(L)$. The 1st subresultant gives $\partial - \phi$ with

$$\begin{aligned}\phi &= \frac{2\mu_1\wp' + 8\lambda\wp^2 - \mu_1\lambda}{2\lambda\wp' + 2\mu_2\wp - \lambda^2} \\ &= \left(\frac{\wp^2 - \frac{\mu_2}{4\lambda}}{\wp^3 - \frac{\mu_2}{4\lambda}\wp^2 + \frac{\mu_1}{4}\wp - \frac{\lambda^2-4}{16}}\right)\wp' + \left(\frac{\frac{\lambda}{2}\wp^2 + \frac{\mu_2}{8}\wp - \frac{\mu}{16\lambda}(\lambda^2 - 4)}{\wp^3 - \frac{\mu_2}{4\lambda}\wp^2 + \frac{\mu_1}{4}\wp - \frac{\lambda^2-4}{16}}\right).\end{aligned}$$

We can now compute $\Psi = \int \Phi dx$ using Maple's integration algorithms. For a complete formula, we refer to the notebook in our public repository (see link above).

Algorithm 1: `BA_Close_Form`

Input : L in $\mathbb{K}[\partial]$ in normal form of order n; of known level M.
Output: BA-function Ψ, or *Error* when L is not algebro-geometric.

$\mathcal{G} \leftarrow$ `Goodearl_Basis`(L, M); `// M used for bounds`
if $\gcd(\mathrm{ord}(A) \ : A \in \{L\} \cup \mathcal{G}) \neq 1$ **then**
  return *Error*;
end
$I \leftarrow$ `BC_ideal`$(L, \mathcal{G})$; `// Provides a Gröbner basis`
$G \leftarrow$element in $\mathcal{G}$ with $(n, \mathrm{ord}(G)) = 1$;
$\mu \leftarrow$variable such that $\phi_L(\mu) = G$;
$SRS \leftarrow$ `Subresultant_Sequence`(L, G);
$Q = \alpha\partial + \beta \leftarrow SRS[1]$; `// Operator of order 1`
$\Phi = -\beta/\alpha$;
$\Psi = \exp\left($`Symbolic_Integrate`$(\Phi)\right)$;
return Ψ;

When L is not algebro-geometric, the algorithm in [5] computes a $C[L]$-basis of a maximal submodule of higher rank. We still compute the BC ideal as in [6] and the greatest common right divisor (now having order higher than one) that determines the BA-function.

Acknowledgements. Both authors have been partially supported by the grant PID2021-124473NB-I00, «Algorithmic Differential Algebra and Integrability» (ADAI) from the Spanish MCIN/AEI /10.13039/501100011033 and by FEDER, UE

References

[1] M. Bronstein: *Symbolic integration I*. Springer Berlin Heidelberg (1997).

[2] R. Delgado, R. Hernández Heredero, A. Jiménez-Pastor, S.L. Rueda, M.Á. Zurro: Computing almost commuting bases of odos and gelfand-dickey hierarchies. *Math. Comput. Sci.* **19**(1), Article no. 4 (2025).

[3] K.R. Goodearl: Centralizers in differential, pseudo-differential and fractional differential operator rings. *Rocky Mountain J. Math.* **13**(4), 573–618 (1983).

[4] A. Jiménez-Pastor, S.L. Rueda: D-Algebra package for SageMath. Zenodo (2025).

[5] A. Jiménez-Pastor, S.L. Rueda: Effective computation of centralizers of odos. *ArXiv:2505.01289* (2025).

[6] A. Jiménez-Pastor, S.L. Rueda: Gröbner bases of burchnall-chaundy ideals for ordinary differential operators. *ArXiv* (2026).

[7] P. Kumbhakar, U. Roy, V.R. Srinivasan: A classification of first order differential equations. *J. Algebra* **644**, 580–608 (2024).

[8] P. Kumbhakar, V.R. Srinivasan: Strongly normal extensions and algebraic differential equations. *ArXiv* (2025).

[9] S.L. Rueda: On the classification of centralizers of odos: An effective differential algebra approach. *ArXiv:2503.03429* (2025).

[10] G. Wilson: *Algebraic curves and soliton equations.* Geometry Today, E. Arbarello et al. (eds.), pages 303–329. Birkhäuser (1985).

Real line congruences of trilinear birational maps

B. Jüttler*, P. Mazón◇†, J. Schicho‡

◇ *Speaker at EACA 2026*

* *Institute of Applied Geometry, Johannes Kepler University*

† *Department of Mathematics, CUNEF Universidad*

‡ *RISC, Johannes Kepler University*

bert.juettler@jku.at, pablo.mazon@cunef.edu, josef.schicho@ricam.oeaw.ac.at

Abstract. Trilinear mappings appear naturally when performing spatial isogeometric discretizations of degree $p = 1$. Among them, birational mappings are characterized by the property that both the mapping and the associated inverse mapping are rational and thus easy to evaluate. These mappings have recently been analyzed by Busé et al. [1]. Among other results, the authors provide a classification of these mappings over the field of complex numbers.

The parameter lines of trilinear mappings form three two-parameter systems of straight lines, and thus it is promising to analyze these mappings with the tools provided by the field of line geometry, which is a classical branch of higher geometry, see [4] for a recent survey. Indeed, in the birational case, the three systems of lines form space-filling line congruences associated with rational mappings that can be used to parameterize certain algebraic surfaces [3]. Moreover, the three systems are closely related, and based on these observations we will present a geometric discussion of the results of Busé et al. [1] together with a more detailed analysis of the classification over the field of real numbers.

Preprint available on: arxiv.org/abs/2603.10666.

Introduction

The goal of this paper is to classify the parametric real line congruences of all possible classes of real trilinear birational maps. These three systems of lines form space-filling line congruences (Definition 1) associated with rational mappings that can be used to parameterize certain algebraic surfaces [3]. Specifically, the space-filling condition on a line congruence L means that for a general $P \in \mathbb{P}^3_{\mathbb{C}}$ we can find a line $\ell \in L$ such that $P \in \ell$.

Real Line Congruences

Let $\mathbb{P}^n_k$ be the projective n-space over a field k. An algebraic variety $X \subset \mathbb{P}^n_{\mathbb{C}}$ is *real* if $X = \overline{X}$, namely it is invariant under complex conjugation. We denote by $X(\mathbb{R})$ its real locus. The set of lines in $\mathbb{P}^3_{\mathbb{C}}$ is an algebraic variety $Q \subset \mathbb{P}(\bigwedge^2 \mathbb{C}^4) \simeq \mathbb{P}(\bigwedge^2 (\mathbb{C}^4)^\vee) \simeq \mathbb{P}^5_{\mathbb{C}}$ of

J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, V. Sotomayor (eds.): Proceedings of the XIX EACA, pp. 171-176 (2026).
ISBN: 978-84-09-87277-0

dimension 4, known as the *Klein quadric*. Specifically, Q is the image of the Grassmannian $\mathrm{Gr}_2(\mathbb{C}^4)$ by the Plücker embedding.

Definition 1. A(n algebraic) *line congruence* is a(n algebraic) surface $S \subset Q \subset \mathbb{P}^5$. It is called *real* if S is real and its real locus $S(\mathbb{R})$ has (real) dimension 2.

There are several ways to specify an algebraic line congruence $S \subset Q$. The two most straightforward approaches are (1) to provide the defining equations of S in $\mathbb{P}^5_{\mathbb{C}}$, or (2) to provide a rational parametrization of S. An intermediate approach, which is often more geometrically intuitive, is (3) to provide a set of focal elements.

Definition 2. Let $S \subset Q$ be a line congruence. A variety $V \subset \mathbb{P}^3_{\mathbb{C}}$ is *focal* for the line congruence S if the following conditions are satisfied:

$a)$ $V \cap \ell \neq \varnothing$ for every $\ell \in S$.
$b)$ V is minimal with respect to property $a)$, i.e. if $W \subset V$ satisfies $a)$ then $W = V$.

Most often, a line congruence is specified by two focal curves. However, in some degenerate cases line congruences can have a single focal point. In our classification, the following line congruences appear.

Definition 3. Let $S \subset Q$ be a real line congruence.

$A.1$. S is *real linear* if it has two distinct skew real focal lines.
$A.2$. S is *complex linear* if it has two distinct skew complex-conjugate focal lines.
B. S is *quadratic* if it has a focal line and a focal plane conic that intersects the line at one point.
C. S is *degenerate* if it has a single focal point.
D. S is *parabolic-linear* if it has a single real focal line (limit case of $A.1$).

Trilinear Birational Maps

Definition 4. A *trilinear rational map* is a rational map

$$\begin{aligned} \phi : (\mathbb{P}^1_{\mathbb{C}})^3 &\dashrightarrow \mathbb{P}^3_{\mathbb{C}} \\ (s_0 : s_1) \times (t_0 : t_1) \times (u_0 : u_1) &\mapsto (f_0 : f_1 : f_2 : f_3) \end{aligned}$$

for some $f_i = f_i(s_0, s_1, t_0, t_1, u_0, u_1)$ trilinear. It is *real* if f_0, f_1, f_2, f_3 are all real. It is *birational* if it admits an inverse rational map.

A real trilinear rational map naturally yields three families of real line congruences. Specifically, these are the three families of parametric lines.

Definition 5. Let ϕ be a real trilinear rational map. An s-line is the image of the restriction of ϕ to $(y_0 : y_1) \times (z_0 : z_1) = (\beta_0 : \beta_1) \times (\gamma_0 : \gamma_1)$, for some point in $\mathbb{P}^1_{\mathbb{C}} \times \mathbb{P}^1_{\mathbb{C}}$. The t- and u-lines are defined analogously.

We denote by S_s, S_t and S_u the line congruences arising respectively as the s-lines, t-lines and u-lines of a trilinear rational map. In the case ϕ is birational, then its inverse is

$$\begin{aligned} \phi^{-1} : \mathbb{P}^3_{\mathbb{C}} &\dashrightarrow \mathbb{P}^1_{\mathbb{C}} \times \mathbb{P}^1_{\mathbb{C}} \times \mathbb{P}^1_{\mathbb{C}} \\ (x_0 : x_1 : x_2 : x_3) &\mapsto (a_0 : a_1) \times (b_0 : b_1) \times (c_0 : c_1) \end{aligned}$$

where $a_i = a_i(x_0, x_1, x_2, x_3)$ (resp. for b_j and c_k) are homogeneous of the same degree without a common factor.

Definition 6. The *type* of a trilinear birational map ϕ is $(\deg a_i, \deg b_j, \deg c_k) \in \mathbb{N}^3$.

The only possible types of a trilinear birational map are (up to permutation of the entries) the following: $(1,1,1)$, $(1,1,2)$, $(1,2,2)$, and $(2,2,2)$.

Classification of Real Line Congruences of Trilinear Birational Maps

In the following, we (1) describe the focal elements of the parametric line congruences of trilinear birational maps, and (2) classify all line congruences for each possible type.

Type $(1,1,1)$

Theorem 7. *Let ϕ be a trilinear birational map of type $(1,1,1)$. Then, we can find lines $a, b, c \subset \mathbb{P}^3_{\mathbb{C}}$ such that:*

1. *The focal varieties of S_s are contained in $b \cup c$.*
2. *The focal varieties of S_t are contained in $a \cup c$.*
3. *The focal varieties of S_u are contained in $a \cup b$.*

Theorem 8. *Let $a, b, c \subset \mathbb{P}^3_{\mathbb{C}}$ be the lines in the statement of* Theorem 7. *Then, $a, b, c \subset \mathbb{P}^3_{\mathbb{R}}$ i.e. they are all real lines. Moreover, any trilinear birational map ϕ of type $(1,1,1)$ falls into one of the following classes:*

1. *The lines a, b, c are pairwise skew, and moreover:*
   (a) *S_s is linear with focal lines b and c.*
   (b) *S_t is linear with focal lines a and c.*
   (c) *S_u is linear with focal lines a and b.*
2. *The lines a, b are coplanar and c is skew to both. Additionally:*
   (a) *S_s is linear with focal lines b and c.*
   (b) *S_t is linear with focal lines a and c.*
   (c) *S_u is degenerate with a single focal point $a \cap b$.*
3. *The lines a, b are skew, and both intersect c. Additionally:*
   (a) *S_s is degenerate with a single focal point $b \cap c$.*
   (b) *S_t is degenerate with a single focal point $a \cap c$.*
   (c) *S_u is linear with focal lines a and b.*
4. *The lines a, b, c are coplanar, and moreover:*

(a) S_s is degenerate with a single focal point $b \cap c$.
(b) S_t is degenerate with a single focal point $a \cap c$.
(c) S_u is degenerate with a single focal point $a \cap b$.

Type $(1,1,2)$

Theorem 9. *Let ϕ be a trilinear birational map of type $(1,1,2)$. Then, we can find two distinct coplanar lines $a, b \subset \mathbb{P}^3_{\mathbb{C}}$ and a plane conic $z \subset \mathbb{P}^3_{\mathbb{C}}$ intersecting both a and b and not lying on the plane spanned by the lines, such that:*

1. *The focal varieties of S_s are contained in $a \cup z$.*
2. *The focal varieties of S_t are contained in $b \cup z$.*
3. *S_u is degenerate with a single focal point $a \cap b$.*

Theorem 10. *Let $a, b, z \subset \mathbb{P}^3_{\mathbb{C}}$ be the lines and plane conic in* Theorem 9*. Then, a, b, z are all real. Moreover, any trilinear birational map ϕ of type $(1,1,2)$ falls into one of the following classes:*

1. *The conic z is smooth and $A \neq B$. Additionally:*
   (a) *S_s is quadratic with focal curves b and z.*
   (b) *S_t is quadratic with focal curves a and z.*
   (c) *S_u is degenerate with a single focal point C.*
2. *The conic z is smooth, $A = B = C$ and the plane spanned by a, b is tangent to z. Additionally:*
   (a) *S_s is quadratic with focal curves b and z.*
   (b) *S_t is quadratic with focal curves a and z.*
   (c) *S_u is degenerate with a single focal point C.*
3. *The conic $z = x \cup y$ is reducible, $A \neq B$, $A \in x$ and $B \in y$. Additionally:*
   (a) *S_s is linear with focal lines b and x.*
   (b) *S_t is linear with focal lines a and y.*
   (c) *S_u is degenerate with a single focal point C.*
4. *The conic $z = x \cup a$ is reducible (hence $A = a \cap z = a$ is a line), $B \in a$ and $B \notin x$. Additionally:*
   (a) *S_s is linear with focal lines b and x.*
   (b) *S_t is parabolic-linear with focal line a.*
   (c) *S_u is degenerate with a single focal point C.*
5. *The conic $z = a \cup b$ is reducible (hence $A = a \cap z = a$ and $B = b \cap z = b$ are lines). Additionally:*
   (a) *S_s is parabolic-linear with focal line b.*
   (b) *S_t is parabolic-linear with focal line a.*
   (c) *S_u is degenerate with a single focal point C.*

Types $(1,2,2)$ and $(2,2,2)$

Due to lack of space, we only summarize the classification results for types $(1,2,2)$ and $(2,2,2)$. For a more detailed account, we refer the reader to [2].

Theorem 11. *The parametric line congruences of a trilinear birational map* $\phi : (\mathbb{P}^1_{\mathbb{C}})^3 \dashrightarrow \mathbb{P}^3_{\mathbb{C}}$ *of type* $(1,2,2)$ *determine:*

a) 8 classes where all the focal varieties are real.
b) 3 classes where some of the focal varieties are nonreal.

Example 12. The trilinear rational map

$$\begin{aligned} \phi : (\mathbb{P}^1_{\mathbb{C}})^3 &\dashrightarrow \mathbb{P}^3_{\mathbb{C}} \\ (s_0 : s_1) \times (t_0 : t_1) \times (u_0 : u_1) &\mapsto (f_0 : f_1 : f_2 : f_3) \end{aligned}$$

with defining polynomials

$$f_0 = s_0t_0u_1 + s_1t_0u_1 + s_0t_1u_1\,, \qquad f_1 = s_1t_0u_1 + s_0t_1u_1 + 2s_1t_1u_1\,,$$

$$f_2 = -s_0t_1u_0 - s_1t_1u_0 + s_0t_0u_1 + s_1t_0u_1\,, \qquad f_3 = -s_1t_1u_0 + s_1t_0u_1$$

admits the inverse

$$\begin{aligned} \phi^{-1} : \mathbb{P}^3_{\mathbb{C}} &\dashrightarrow (\mathbb{P}^1_{\mathbb{C}})^3 \\ (x_0 : x_1 : x_2 : x_3) &\mapsto (\sigma_0 : \sigma_1) \times (\tau_0 : \tau_1) \times (\upsilon_0 : \upsilon_1) \end{aligned}$$

given by

$$\sigma_0 = x_2 - x_3\,, \qquad \sigma_1 = x_3\,,$$

$$\tau_0 = x_0x_2 - x_1x_2 + x_0x_3 + x_1x_3\,, \qquad \tau_1 = x_1x_2 - x_0x_3\,,$$

$$\upsilon_0 = x_0x_2 - x_1x_2 - x_2^2 + x_0x_3 + x_1x_3 - x_3^2\,, \qquad \upsilon_1 = x_1x_2 - x_0x_3\,.$$

Hence, ϕ is birational of type $(1,2,2)$. Moreover, the focal varieties consist of:

1. Three real lines $a, b, c \subset \mathbb{P}^3_{\mathbb{C}}$.
2. Two skew complex-conjugate lines $x, y \subset \mathbb{P}^3_{\mathbb{C}}$.

Theorem 13. *The parametric line congruences of a trilinear birational map* $\phi : (\mathbb{P}^1_{\mathbb{C}})^3 \dashrightarrow \mathbb{P}^3_{\mathbb{C}}$ *of type* $(2,2,2)$ *determine 2 classes where all the focal varieties are real.*

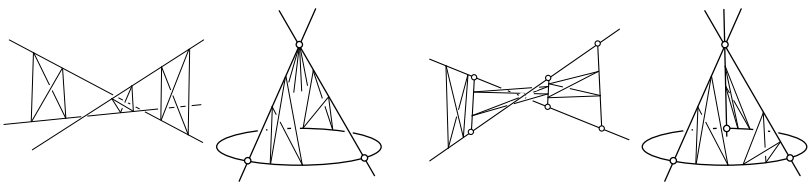


Figure 1. The focal varieties of the parametric real line congruences of the general class of types, from left to right, $(1,1,1)$, $(1,1,2)$, $(1,2,2)$, $(2,2,2)$.

Acknowledgements. The second author was partially supported by the PRIN 2022 under the grant agreement 40104520.

References

[1] L. Busé, P. González-Mazón, J. Schicho: Trilinear birational maps in dimension three. *Math. Comp.* **92**(342), 1837–1866 (2023).

[2] B. Jüttler, P. Mazón, J. Schicho: Real line congruences of trilinear birational maps. *ArXiv:2603.10666* (2026).

[3] B. Jüttler, K. Rittenschober: *Using line congruences for parameterizing special algebraic surfaces*. Mathematics of Surfaces, 223–243. Springer (2003).

[4] H. Pottmann, J. Wallner: *Computational line geometry*. Springer (2001).

Optimisation on constant-torsion polygonal curves

S. Kaji[◇*], N. Matsuura[†], S. Shigetomi[‡]

[◇] *Speaker at EACA 2026*

[*] *Graduate School of Science, Kyoto University*

[†] *Department of Applied Mathematics, Fukuoka University*

[†] *Institute of Mathematics for Industry, Kyushu University*

kaji.shizuo.7r@kyoto-u.ac.jp, nozomu@fukuoka-u.ac.jp, s-shigetomi@imi.kyushu-u.ac.jp

Abstract. We study a class of closed polygonal curves in $\mathbb{R}^3$ with constant torsion, which provides a mathematical model for a class of rotatable origami mechanisms known as kaleidocycles. The configuration space of such curves is described as a real algebraic set defined by quadratic equations arising from closure and constant-torsion constraints. We investigate the existence and mobility of kaleidocycles via these configuration spaces as functions of the number of edges and the torsion parameter. Moreover, we address design problems formulated as constrained optimisation on these configuration spaces. Several open questions and computational challenges are presented.

Introduction

Closed polygonal curves with constant torsion arise naturally in the study of discrete differential geometry and linkage mechanisms. In particular, they provide a mathematical model for rotatable origami rings known as *kaleidocycles*. These mechanisms consist of a cyclic chain of hinged tetrahedral modules that exhibit a smooth rotational motion.

From a geometric viewpoint, a kaleidocycle can be described by a closed discrete space curve whose binormal vectors satisfy constant-angle conditions. This formulation leads to a real algebraic configuration space defined by quadratic constraints. Understanding the structure of this space is essential both for the geometric analysis of the mechanism and for solving practical design problems.

The purpose of this extended abstract is twofold. First, we describe a quadratic formulation of the configuration space of constant-torsion polygonal curves. Second, we discuss optimisation problems on this space motivated by the design of kaleidocycles with minimal twist and smooth mobility.

Quadratic formulation of the configuration space

A closed polygonal curve in $\mathbb{R}^3$ with N unit-length edges is given by a map

$$\gamma\colon \{0,1,\dots,N\} \to \mathbb{R}^3, \qquad \gamma_0 = \gamma_N, \qquad \|\gamma_{i+1} - \gamma_i\| = 1.$$

J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, V. Sotomayor (eds.): Proceedings of the XIX EACA, pp. 177-181 (2026).
ISBN: 978-84-09-87277-0

Here we write $\gamma_i := \gamma(i)$ and interpret indices modulo N. Let t_i denote the unit tangent vector of the i-th edge:

$$t_i = \gamma_{i+1} - \gamma_i.$$

At each vertex $i \in \{0, 1, \ldots, N\}$, choose a unit binormal vector b_i orthogonal to the adjacent tangent vectors t_{i-1} and t_i. With this choice of binormals, the (signed) curvature angle $\kappa_i \in (-\pi, \pi]$ and torsion angle $\mu_i \in [0, \pi]$ at vertex i are defined by

$$\langle t_{i-1}, t_i \rangle = \cos \kappa_i, \qquad \langle b_{i-1}, b_i \rangle = \cos \mu_i.$$

The sign of κ_i is positive if $\langle t_i, b_i \times b_{i+1} \rangle > 0$.

We fix a torsion parameter $\mu \in (0, \pi)$ and let $c = \cos \mu$. We consider the set of vectors $b_0, \ldots, b_N \in \mathbb{R}^3$ satisfying the following system of quadratic equations:

$$b_N = -b_0, \quad \sum_{i=1}^{N} (b_{i-1} \times b_i) = 0, \quad \langle b_i, b_{i+1} \rangle = c, \quad \langle b_i, b_i \rangle = 1 \quad (0 \le i < N). \tag{1}$$

These constraints define a closed polygonal curve with constant torsion by

$$\gamma_i = \frac{1}{\sin \mu} \sum_{j=1}^{i} (b_{j-1} \times b_j),$$

where the binormal vectors of γ coincide with the sequence $\{b_i \mid 0 \le i \le N\}$.

We denote by $\mathcal{M}_{N,c}$ the corresponding real algebraic set modulo the $O(3)$-symmetry induced by the simultaneous rotation or reflection of all b_i. These curves model a specific class of rotatable origami mechanisms known as kaleidocycles (see Figure 1) [7, 8], which may be regarded as discrete analogues of uniformly twisted Möbius strips.

Two fundamental questions concerning $\mathcal{M}_{N,c}$ are:

1. **Existence:** For which pairs (N, c) is $\mathcal{M}_{N,c}$ non-empty?
2. **Mobility:** When non-empty, what are the dimension and global structure of $\mathcal{M}_{N,c}$?

Partial answers are provided by the following theorem.

Theorem 1 ([6, 7]). *1. There exists a flow on $\mathcal{M}_{N,c}$ defined by a semi-discrete analogue of the mKdV/sine-Gordon equations.*

2. For any $N \ge 6$, there exists a one-dimensional component of $\mathcal{M}_{N,c}$ for some $c \ne \pm 1$, which coincides with a trajectory of this flow.

Optimisation on the configuration space

For a fixed N, one design objective is to minimise the torsion angle μ –or equivalently, to maximise $c = \cos \mu$– subject to the constraints defining $\mathcal{M}_{N,c}$. This corresponds to constructing a discrete Möbius strip with minimal twist. The resulting constrained optimisation problem is

$$\max c \quad \text{subject to} \quad (b_0, \ldots, b_N) \in \mathcal{M}_{N,c}. \tag{2}$$

To account for the topology of a Möbius strip, we allow b_0 and b_N (and hence κ_0 and κ_N) to have opposite signs.

In our numerical and physical experiments, we observed that kaleidocycles with minimal torsion angle exhibit single-degree-of-freedom motions. This motivates the following conjecture:

Conjecture 2. *For any $N \geq 6$, if c_* attains the maximum in* (2)*, then $\mathcal{M}_{N,c_*}$ is homeomorphic to S^1.*

The expected dimension of $\mathcal{M}_{N,c}$ is given by the Kutzbach–Grübler formula from mechanism theory (see e.g. [5]):

$$3N - (3 + N + N) - 3 = N - 6.$$

This count accounts for $3N$ variables, 3 closure constraints, N unit length constraints, N angle constraints, and the 3-dimensional $O(3)$-symmetry. The conjecture asserts that this generic count fails at the optimal value c_*, resulting in a pure rotational motion without wobble. When $N \geq 8$, such behaviour corresponds to a rare type of underconstrained mechanism and has been patented [8].

While a space curve is determined by its curvature and torsion up to rigid motion, Problem (2) concerns only torsion. We therefore consider a secondary optimisation problem involving curvature:

$$\min \sum_{i=0}^{N-1} \log\bigl(1 + \tan^2(\kappa_i/2)\bigr) \quad \text{subject to} \quad (b_0, \ldots, b_N) \in \mathcal{M}_{N,c}. \tag{3}$$

Using the identity

$$\log(1 + \tan^2(\alpha/2)) = \log 2 - \log(1 + \cos\alpha),$$

the optimisation problem is equivalent to maximising $\sum \log(1 + \cos\kappa_i)$.

The functional in (3) represents a discrete analogue of elastic bending energy [3]. Although curvature and torsion are locally independent, the global closure condition couples them, leading to the following conjecture.

Conjecture 3. *For any $N \geq 6$, if c_* attains the maximum in* (2)*, then the same configuration also attains the minimum in (3).*

Supporting evidence is provided by the following result.

Proposition 4. *The elastic energy in (3) is invariant under the flow described in Theorem 1.*

Additional conserved quantities arise from topology. By the Călugăreanu–White theorem [4],

$$\mathrm{Lk} = 2(\mathrm{Tw} + \mathrm{Wr})$$

takes integer values. In the discrete setting, it may be expressed as ([1])

$$\mathrm{Lk} = \frac{1}{\pi}\sum_{i=1}^{N} \mu_i + \frac{1}{\pi} \sum_{0 \leq i < j < N} \Omega(i, j),$$

The standard linking number is given by $\mathrm{Tw} + \mathrm{Wr}$. To adapt this to the Möbius topology, we instead consider the doubled quantity.

where $\Omega(i,j)$ is the signed solid angle subtended by the i-th and j-th edges. This integer corresponds to the number of half-twists in the associated Möbius strip and is necessarily odd because $b_0 = -b_N$.

In the smooth setting, the uniformly twisted minimal Möbius strip has Lk $= 1$. However, computational experiments suggest that no discrete counterpart exists.

Conjecture 5. *For any $N \geq 6$, there exists no solution of* (1) *with* Lk $= 1$.

In principle, this problem is decidable via quantifier elimination using the Tarski–Seidenberg theorem (see e.g. [2]), but the computational complexity becomes prohibitive as N increases.

The computer code used to numerically verify these conjectures is available online (see `https://github.com/shizuo-kaji/Kaleidocycle`).

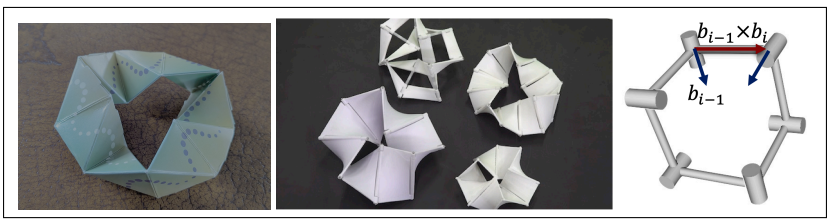


Figure 1. Examples of kaleidocycles and the correspondence to a closed curve.

Acknowledgements. The first author has been partially supported by JSPS KAKENHI 25K00921 and 25H00399. The second author has been partially supported by JSPS KAKENHI 25K00921 and 23K03125. The third author has been partially supported by JSPS KAKENHI 25K00921 and 25K17297.

References

[1] P.K. Agarwal, H. Edelsbrunner, Y. Wang: Computing the writhing number of a polygonal knot. *Discrete Comput. Geom.* **32**(1), 37–53 (2004).

[2] S. Basu, R. Pollack, M.F. Roy: *Algorithms in Real Algebraic Geometry*. Springer (2006).

[3] A.I. Bobenko, Y.I. Suris: Discrete time Lagrangian mechanics on Lie groups, with an application to the Lagrange top. *Comm. Math. Phys.* **204**, 147–188 (1999).

[4] M.R. Dennis, J.H. Hannay: Geometry of Călugăreanu's theorem. *Proc. R. Soc. A* **461**(2062), 3245–3254 (2005).

[5] K.H. Hunt: *Kinematic Geometry of Mechanisms*. Oxford University Press (1978).

[6] S. Kaji, K. Kajiwara, H. Park: *Linkage mechanisms governed by integrable deformations of discrete space curves*. Nonlinear systems and their remarkable mathematical structures **2**, 356–381. CRC Press (2019).

[7] S. Kaji, K. Kajiwara, S. Shigetomi: An explicit construction of kaleidocycles by elliptic theta functions. *ArXiv:2308.04977* (2023).

[8] S. Kaji, J. Schönke, E. Fried, M. Grunwald: Moebius kaleidocycle. Japanese Patent JP7261490 (2018).

Radical splittings of toric ideals

A. Katsampekis[◇*], A. Thoma[*]

[◇] *Speaker at EACA 2026*

[*] *Department of Mathematics, University of Ioannina*

katsampekis@uoi.gr, athoma@uoi.gr

Abstract. Let $I_A \subset K[x_1, \ldots, x_n]$ be a toric ideal. In this paper, we give a necessary and sufficient condition for the toric variety $V(I_A)$, over an algebraically closed field, to be expressed as the set-theoretic intersection of other toric varieties. We also introduce the radical splitting number of I_A, denoted by $\text{Split}_{\text{rad}}(I_A)$, and compute its exact value in several cases, with particular emphasis on toric ideals arising from graphs. In particular, we show that $\text{Split}_{\text{rad}}(I_A) = 3$ for toric ideals of complete bipartite graphs. Additionally, we prove that $\text{Split}_{\text{rad}}(I_A)$ coincides with the binomial arithmetical rank of I_A when the height of I_A equals 2. A complete version of this work appears as a preprint on arXiv [8].

Introduction

A natural question in algebraic geometry is to determine when an affine algebraic variety $V \subset K^n$ can be expressed as the intersection of two distinct affine algebraic varieties, V_1 and V_2, over an algebraically closed field K; that is, $V = V_1 \cap V_2$, with $V \subsetneqq V_i$ for $1 \leq i \leq 2$. This geometric question translates algebraically via the Hilbert Nullstellensatz into an ideal-theoretic question:

$$I(V) = \text{rad}(I(V_1) + I(V_2)),$$

where $I(W)$ denotes the ideal of an affine algebraic variety W and $\text{rad}(J)$ is the radical of an ideal J, see [1, Chapter 4]. This paper addresses the latter problem in the case where all varieties involved are toric varieties. In other words, we study when a given toric ideal $I_A \subset K[x_1, \ldots, x_n]$ can be written as $I_A = \text{rad}(I_{A_1} + I_{A_2})$ and $I_{A_i} \subsetneqq I_A$ for $1 \leq i \leq 2$. Recent advances in understanding toric splittings [2, 3, 6, 7], along with several earlier results on the binomial generation of toric ideals up to radical [4, 5], allow us to provide a necessary and sufficient condition for the equality $I_A = \text{rad}(I_{A_1} + I_{A_2})$.

Let $A = \{\mathbf{a}_1, \ldots, \mathbf{a}_n\}$ be a vector configuration in $\mathbb{Z}^m$, $\ker_{\mathbb{Q}}(A) = \{\mathbf{u} = (u_1, \ldots, u_n) \in \mathbb{Q}^n \mid u_1\mathbf{a}_1 + \cdots + u_n\mathbf{a}_n = \mathbf{0}\}$, and $\ker_{\mathbb{Z}}(A) = \ker_{\mathbb{Q}}(A) \cap \mathbb{Z}^n$. Throughout this paper, we will assume that the affine semigroup $\mathbb{N}A = \{l_1\mathbf{a}_1 + \cdots + l_n\mathbf{a}_n \mid l_i \in \mathbb{N}\}$ is pointed; namely $\ker_{\mathbb{Z}}(A) \cap \mathbb{N}^n = \{\mathbf{0}\}$. Consider the polynomial ring $K[x_1, \ldots, x_n]$ over a field K. The *toric ideal* I_A is the kernel of the K-algebra homomorphism $\phi : K[x_1, \ldots, x_n] \longrightarrow K[t_1, \ldots, t_m, t_1^{-1}, \ldots, t_m^{-1}]$ given by $\phi(x_i) = \mathbf{t}^{\mathbf{a}_i}$ for all $i = 1, \ldots, n$ and it is generated

J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, V. Sotomayor (eds.): Proceedings of the XIX EACA, pp. 182-186 (2026).
ISBN: 978-84-09-87277-0

by all the binomials $B(\mathbf{u}) := \mathbf{x}^{\mathbf{u}^+} - \mathbf{x}^{\mathbf{u}^-}$ such that $\mathbf{u}^+ - \mathbf{u}^- \in \ker_{\mathbb{Z}}(A)$, where $\mathbf{u}^+ \in \mathbb{N}^n$ and $\mathbf{u}^- \in \mathbb{N}^n$ denote the positive and negative part of $\mathbf{u} = \mathbf{u}^+ - \mathbf{u}^-$, respectively (see, for instance, [9, Lemma 4.1]). The set $V(I_A) = \{(u_1, \dots, u_n) \in K^n \mid F(u_1, \dots, u_n) = 0, \forall F \in I_A\}$ of zeroes of I_A is called *affine toric variety*, which is not necessarily normal.

Definition 1. Let I_A be a toric ideal.

1. The *splitting number* of I_A, denoted by $\mathrm{Split}(I_A)$, is the smallest integer s such that $I_A = I_{A_1} + \cdots + I_{A_s}$ and $I_{A_i} \neq I_A$ for every $1 \leq i \leq s$.
2. The *radical splitting number* of I_A, denoted by $\mathrm{Split}_{\mathrm{rad}}(I_A)$, is the smallest integer r such that $I_A = \mathrm{rad}(I_{A_1} + \cdots + I_{A_r})$ and $I_{A_i} \neq I_A$ for every $1 \leq i \leq r$.

Remark 2. (1) Since I_A is minimally generated by binomials, we get that $\mathrm{Split}(I_A) \leq \mu(I_A)$, where $\mu(I_A)$ is the minimal number of generators of I_A.
(2) The invariant $\mathrm{Split}(I_A)$ is an upper bound for $\mathrm{Split}_{\mathrm{rad}}(I_A)$.

The *binomial arithmetical rank* of I_A, denoted by $\mathrm{bar}(I_A)$, is the smallest integer t for which there exist binomials $B_1, \dots, B_t$ in I_A such that $I_A = \mathrm{rad}(B_1, \dots, B_t)$. From the generalized Krull's principal ideal theorem, we deduce that the height $\mathrm{ht}(I_A)$ of I_A is a lower bound for $\mathrm{bar}(I_A)$. From the definitions, we obtain the following inequalities for a non-principal toric ideal I_A:

$$2 \leq \mathrm{Split}_{\mathrm{rad}}(I_A) \leq \mathrm{bar}(I_A) \leq \mu(I_A).$$

In Section 1, we provide a necessary and sufficient condition for a toric ideal I_A to satisfy $\mathrm{Split}_{\mathrm{rad}}(I_A) = 2$ (see Corollary 4). We also show that this equality holds when $\mathrm{ht}(I_A) \geq 3$ and $\mathrm{bar}(I_A) \leq 2r - 2$ (see Theorem 5), or when $\mathrm{ht}(I_A) \geq 3$ and I_A is the defining ideal of a simplicial toric variety with full parametrization (see Proposition 6).

In Section 2, we show that for a bipartite graph G, the toric ideal I_G satisfies $\mathrm{Split}(I_G) = \mathrm{Split}_{\mathrm{rad}}(I_G)$ (see Theorem 7). Moreover, we show that $\mathrm{Split}_{\mathrm{rad}}(I_G) = 3$ for a complete bipartite graph G (see Theorem 8). We also study the special case in which I_A is a toric ideal of height 2. In this setting, we show that $\mathrm{Split}(I_A) = \mu(I_A)$ and $\mathrm{Split}_{\mathrm{rad}}(I_A) = \mathrm{bar}(I_A)$ (see Theorem 9). Furthermore, we explicitly compute the splitting and the radical splitting number of the toric ideal $I_{\Lambda(A)}$ (see Proposition 11), where $\Lambda(A)$ is the Lawrence lifting of the vector configuration A associated with a symmetric monomial curve in $\mathbb{P}^3$. Proposition 11 shows that the splitting number can be arbitrarily large for some configurations, while the radical splitting number remains constant for them. Finally, we show that both $\mathrm{Split}(I_A)$ and $\mathrm{Split}_{\mathrm{rad}}(I_A)$ can be arbitrarily large for certain other configurations; see Proposition 12.

Radical Splitting Criterion for I_A

Let $A = \{\mathbf{a}_1, \dots, \mathbf{a}_n\}$ be a vector configuration in $\mathbb{Z}^m$. Given a set $C = \{\mathbf{c}_1, \dots, \mathbf{c}_k\} \subset \mathbb{Z}^n$, let $\mathrm{span}_{\mathbb{Q}}(C) = \{\lambda_1\mathbf{c}_1 + \cdots + \lambda_k\mathbf{c}_k \mid \lambda_i \in \mathbb{Q}\}$ be the $\mathbb{Q}$-vector space generated by the vectors of C. A set S is a *minimal system of binomial generators* of the toric ideal I_A *up to radical* if there exist no $S' \subsetneq S$ such that S' generate I_A up to radical.

Theorem 3. *There are toric ideals I_{A_i} with $I_{A_i} \neq I_A$ for every $1 \leq i \leq s$, such that $I_A = I_{A_1} + \cdots + I_{A_s}$ (respectively, $I_A = \mathrm{rad}(I_{A_1} + \cdots + I_{A_s})$) if and only if there exists a minimal system of binomial generators $\{B(\mathbf{u}) \mid \mathbf{u} \in C \subset \ker_{\mathbb{Z}}(A)\}$ of the toric ideal I_A (respectively, of I_A up to radical), and sets C_i, $1 \leq i \leq s$, such that $C = \cup_{i=1}^{s} C_i$ and $\mathrm{span}_{\mathbb{Q}}(C_i) \subsetneqq \ker_{\mathbb{Q}}(A)$ for every $1 \leq i \leq s$.*

The next corollary is derived directly from Theorem 3 for $s = 2$.

Corollary 4. *There are toric ideals I_{A_i} with $I_{A_i} \neq I_A$ for every $1 \leq i \leq 2$, such that $I_A = \mathrm{rad}(I_{A_1} + I_{A_2})$ if and only if there exists a minimal system of binomial generators $\{B(\mathbf{u}) \mid \mathbf{u} \in C \subset \ker_{\mathbb{Z}}(A)\}$ of the toric ideal I_A if and only if there exists a minimal system of binomial generators $\{B(\mathbf{u}) \mid \mathbf{u} \in C \subset \ker_{\mathbb{Z}}(A)\}$ of the toric ideal I_A up to radical, and sets C_1 and C_2 such that $C = C_1 \cup C_2$, $\mathrm{span}_{\mathbb{Q}}(C_1) \subsetneqq \ker_{\mathbb{Q}}(A)$, and $\mathrm{span}_{\mathbb{Q}}(C_2) \subsetneqq \ker_{\mathbb{Q}}(A)$.*

The following theorem establishes that $\mathrm{Split}_{\mathrm{rad}}(I_A) = 2$ whenever $\mathrm{bar}(I_A) \leq 2\mathrm{ht}(I_A) - 2$, provided that $\mathrm{ht}(I_A) \geq 3$.

Theorem 5. *If I_A is a toric ideal of height $r \geq 3$ such that its binomial arithmetical rank is less than or equal to $2r - 2$, then $\mathrm{Split}_{\mathrm{rad}}(I_A) = 2$.*

Let $d_1, \ldots, d_n$ be positive integers and $a_{i,j}$ be integers, where $1 \leq i \leq r$, $1 \leq j \leq n$ and for all $i = 1, \ldots, r$ at least one of $a_{i,1}, \ldots, a_{i,n}$ is nonzero. Let A be the set of columns of the matrix

$$\begin{pmatrix} d_1 & 0 & \cdots & 0 & a_{1,1} & \cdots & a_{r,1} \\ 0 & d_2 & \cdots & 0 & a_{1,2} & \cdots & a_{r,2} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & d_n & a_{1,n} & \cdots & a_{r,n} \end{pmatrix},$$

and let $I_A \subset K[x_1, \ldots, x_{n+r}]$ be the corresponding toric ideal of height r. The toric variety $V(I_A) \subset K^{n+r}$ is called *simplicial* if $a_{i,j} \geq 0$ for all $1 \leq i \leq r$ and $1 \leq j \leq n$. We say that a simplicial toric variety $V(I_A) \subset K^{n+r}$ has a *full parametrization* if $a_{i,j} \neq 0$ for all (i, j).

Proposition 6. *Let K be a field of any characteristic and let $V(I_A) \subset K^{n+r}$ be a simplicial toric variety with full parametrization, where $\mathrm{ht}(I_A) = r \geq 3$. Then $\mathrm{Split}_{\mathrm{rad}}(I_A) = 2$.*

Applications

Let G be a finite, simple, connected graph in the vertex set $\{v_1, \ldots, v_m\}$ with the edge set $E(G) = \{e_1, \ldots, e_n\}$. For each edge $e = \{v_i, v_j\}$ of G, we associate a vector $\mathbf{a}_e \in \{0, 1\}^m$ defined as follows: the ith entry of $\mathbf{a}_e$ is 1, the jth entry is 1, and all other entries are zero. We denote the toric ideal I_{A_G} in $K[e_1, \ldots, e_n]$ by I_G, where $A_G = \{\mathbf{a}_e \mid e \in E(G)\} \subset \mathbb{N}^m$.

Theorem 7. *Let G be a bipartite graph, then $\mathrm{Split}(I_G) = \mathrm{Split}_{\mathrm{rad}}(I_G)$.*

A bipartite graph G is called a *complete bipartite* graph if its vertex set can be partitioned into two subsets V_1 and V_2 such that every vertex of V_1 is connected to every vertex of V_2. It is denoted by $K_{m,n}$, where m and n are the numbers of vertices in V_1 and V_2 respectively. The following theorem explicitly computes the radical splitting number of $I_{K_{m,n}}$.

Theorem 8. *The splitting number and the radical splitting number of the toric ideal of a complete bipartite graph $K_{m,n}$ are both equal to three, where $m, n \geq 2$ and $(m, n) \neq (2, 2)$.*

Next, we study the special case in which $I_A \subset K[x_1, \ldots, x_n]$ is a toric ideal of height 2.

Theorem 9. *Let I_A be a toric ideal of height 2. Then* $\mathsf{Split}(I_A) = \mu(I_A)$ *and* $\mathsf{Split}_{\mathsf{rad}}(I_A) = \mathsf{bar}(I_A)$.

The corollary below gives bounds for $\mathsf{Split}_{\mathsf{rad}}(I_A)$ when $V(I_A)$ is a simplicial toric variety.

Corollary 10. *Let $V(I_A)$ be a simplicial toric variety, where I_A is a toric ideal of height 2. Then $2 \leq \mathsf{Split}_{\mathsf{rad}}(I_A) \leq 3$.*

Let $a < b < d$ be positive integers with $\gcd(a, b, d) = 1$ and $a + b = d$, and let A be the set of columns of the 2×4 matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & a & b & a+b \end{pmatrix}.$$

The Lawrence lifting $\Lambda(A)$ of A is the set of columns of the 6×8 matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & a & b & a+b & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Proposition 11. *For the Lawrence lifting $\Lambda(A)$ of A, the following statements hold:*

1. *The splitting number of $I_{\Lambda(A)}$ is $a + b + 2$.*
2. *The radical splitting number of $I_{\Lambda(A)}$ is 4.*

Given an integer t, define

$$\mathbf{a}_t = \begin{pmatrix} 1 \\ t \\ t^2 \\ \vdots \\ t^{2d-2} \end{pmatrix} \in \mathbb{Z}^{2d-1},$$

where $d \geq 2$ is an integer. Let A denote the cyclic configuration formed by the columns of the $(2d-1) \times (2d+1)$ Vandermonde matrix $\begin{pmatrix} \mathbf{a}_{t_1} & \mathbf{a}_{t_2} & \cdots & \mathbf{a}_{t_{2d+1}} \end{pmatrix}$, where $t_1 < t_2 < \cdots < t_{2d+1}$ are integers.

Proposition 12. *Let I_A be the toric ideal of a cyclic configuration of height two. The splitting number and the radical splitting number of I_A can attain arbitrarily large values.*

References

[1] D. Cox, J. Little, D. O'Shea: *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. 3rd Edition, Springer (2006).

[2] G. Favacchio, J. Hofscheier, G. Keiper, A. Van Tuyl: Splittings of toric ideals. *J. Algebra* **574**, 409–433 (2021).

[3] P. Gimenez, H. Srinivasan: Gluing and splitting of homogeneous toric ideals. *J. Algebra* **667**, 911–930 (2025).

[4] A. Katsabekis: On the binomial arithmetical rank of toric ideals. *J. Algebra Appl.* **13**, 1450030 (2014).

[5] A. Katsabekis, M. Morales, A. Thoma: Binomial generation of the radical of a lattice ideal. *J. Algebra* **324**, 1334–1346 (2010).

[6] A. Katsabekis, A. Thoma: Splittings of toric ideals of graphs. *J. Algebraic Combin.* **61**, Paper No. 16 (2025).

[7] A. Katsabekis, A. Thoma: Toric splittings. *J. Pure Appl. Algebra* **229**, 107870 (2025).

[8] A. Katsabekis, A. Thoma: Radical splittings of toric ideals. *ArXiv:2507.15785* (2026).

[9] B. Sturmfels: *Gröbner Bases and Convex Polytopes*. University Lecture Series **8**, MAS (1995).

Linear complementary pairs of skew BCH constacyclic codes

F.J. Lobillo*, J.M. Muñoz◇

◇ *Speaker at EACA 2026*

* *IMAG, CITIC and Department of Algebra, University of Granada*

jlobillo@ugr.es, munoz@ugr.es

Abstract. Linear complementary pairs (LCPs) of codes were proposed as a countermeasure against potential hardware attacks on integrated circuits, such as hardware Trojan horses, side channel attacks, fault injection attacks and probe attacks. The state of the integrated circuit can be encoded using one of the codes in an LCP and masked by a random codeword from the other code. This results in a security parameter, which is the minimum number of bits that any attack has to read or write in order to have a nonzero probability of being successful, and follows from the minimum Hamming distance of codes. As the original proposal for constructing LCPs of codes considers computing the minimum Hamming distance of randomly generated codes, it is highly inefficient in finding pairs of codes with high security parameter, in the sense of being close to the optimal minimum distance of comparable codes. Another approach is to construct codes which, by design, reach a prescribed security parameter. For this, we consider skew BCH constacyclic codes. The construction of LCPs of codes from them is remarkably simple, and these codes have an additional advantage in that any word can be checked to be a codeword using an algebraic procedure, without the need of implicitly storing a parity check matrix in the integrated circuit, potentially resulting in a smaller overhead for the resulting integrated circuit.

The hardware problem

As the production of integrated circuits is often outsourced, and therefore they have to be transported, there is an interest in being able to detect whether any given integrated circuit has been compromised, at some point before the final delivery, by adding any unplanned component, in what constitutes a hardware attack. For example, a malicious device could be reading the state of the integrated circuit in order to extract information (*probe attack*), or might randomly write into the state of the integrated circuit in order to cause it to misbehave or halt, potentially leading to the inference of some information from the resulting behaviour (*fault injection attack*, FIA). A particular type of attack, which is the *hardware Trojan horse* (HTH), waits until the state of the integrated circuit satisfies some given condition, and then performs an action on the circuit or the device. These attacks might not be detected until a large batch of compromised devices has been delivered. Furthermore, these attacks can be deeply merged into the integrated circuit (for example, as a redesign

J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, V. Sotomayor (eds.): Proceedings of the XIX EACA, pp. 187-191 (2026).
ISBN: 978-84-09-87277-0

of the integrated circuit itself), so repairing the device by removing the malicious parts might be impossible, and detecting the attack by inspecting the integrated circuit or the device might be impractical as the result might be hardly distinguishable from the uncompromised version.

These attacks might be caught by reading information on the integrated circuit (or some point thereof, or a larger segment of the device), such as the weight, temperature, energy consumption, delay between operations, or magnetic leakage. If the measured values do not match the expected ones, an attack can be suspected. However, *side channel attacks* (SCAs) consist of actually reading such kind of information. Both SCAs and probing attacks can be especially concerning against integrated circuits known to process sensitive information, such as non-public keys in a cryptographic scheme.

A solution to the hardware problem: LCPs of codes

In order to force these attacks to be more difficult and detectable, [2] proposes encoding the state of the integrated circuit by using a binary code and masking it by adding a pseudo-random vector of bits. The state of the circuit has to be identifiable by the circuit itself, so the added bits must belong to a supplementary vector space from the code. Hence, if the integrated circuit has a state of k bits and is encoded into a state of $n \geq k$ bits, then each state of the circuit is encoded by using some $[n, k]$ binary code $\mathcal{C}$ and masked by using a pseudo-random codeword in an $[n, n-k]$ code $\mathcal{D}$ such that $\mathcal{C} \oplus \mathcal{D} = \mathbb{F}_2^n$. Thus, each encoded and masked state represents a single state in the original integrated circuit. The encoded circuit is itself an integrated circuit and can therefore be optimized by, for example, removing redundant logic gates. This obfuscates the encoding logic with the logic of the original circuit and reduces the overhead of encoding.

This procedure of encoding and masking results in the absence of a one-to-one correspondence between the state of the (encoded) circuit and the state of the original circuit. Hence, an unintended observer will not be able to infer that the circuit is in the same state in any two moments in time unless either they know how the encoding works or the pseudo-random element happens to be the same. This also protects from SCAs by reducing the distinguishability of different states of the circuit. Furthermore, any observer (such as one performing a probing attack or a HTH) will not be able to make any inference on the state of the circuit unless enough bits have been read, while reading any bit on the unencoded circuit does give some information. Specifically, if the minimum Hamming distance of the dual code of $\mathcal{D}$, $(\mathcal{D})^{\perp}$, is d_{Trigger}, then reading less than d_{Trigger} bits of the encoded circuit will provide no information whatsoever on the (decoded) state. Similarly, in order to get the circuit into a distinct state (as intended in a HTH or a FIA), the number of bits to be modified is at least d_{Payload}, defined as the minimum Hamming distance of $\mathcal{C}$, as the encoded state of the circuit will otherwise not be the one for another state with the same mask. Before generating the next new mask, the circuit can check at each step whether the encoded state of the circuit requires the current mask. Otherwise, it can launch a handling procedure in order to avoid the attack (or a hardware error) and the possible consequences of the invalid state. While an attack can be successful by reading or writing all the bits of the encoded

circuit (and understanding the encoding logic), accessing all bits requires a more substantial modification of the integrated circuit or its surroundings, so a compromised circuit or device is easier to identify. The *security parameter* is defined as the minimum of d_{Trigger} and d_{Payload}, that is, the minimum number of bits that any such attack has to be able to read or write in order to have a nonzero success chance.

While [2] considers binary codes, the generalization to any field F is straightforward.

Definition 1. A pair of codes $(\mathcal{C}, \mathcal{D})$, where each code is a vector subspace of F^n for some field F, is a *linear complementary pair (LCP) of codes* when $\mathcal{C} \oplus \mathcal{D} = F^n$.

Definition 2. The *security parameter* of a pair of linear codes $(\mathcal{C}, \mathcal{D})$ in a common vector space F^n is the minimum of the minimum Hamming distance of $\mathcal{C}$ and the one of $\mathcal{D}^\perp$.

The original proposal in [2] for getting LCPs of codes is to choose either $\mathcal{C}$ or $\mathcal{D}^\perp$ as a code with a good known minimum Hamming distance, and then randomly generate the remaining member, computing the resulting security parameter, and trying again if it is unsatisfactory. This approach has a major problem in the fact that randomly generated codes will almost certainly have unsatisfactory minimum Hamming distances (in the sense that they will be well below the optimal ones) and, furthermore, computing the minimum distance of a general code is a computationally hard task. Hence, this proposal has to compromise either d_{Trigger} or d_{Payload}, and as a result the whole security parameter.

Another approach is to take advantage of the knowledge of some family of codes by choosing both $\mathcal{C}$ and $\mathcal{D}^\perp$ as code with a prescribed, satisfactory minimum Hamming distance, or a lower bound thereof. In this work, we consider skew BCH constacyclic codes.

Skew constacyclic codes

Skew polynomial rings are a particular case of Ore polynomial rings.

Definition 3. The *skew polynomial ring* over the field F, the field automorphism $\sigma : F \to F$ and the variable x, denoted by $F[x;\sigma]$, is the set of polynomials over x (where x is on the right) with coefficients in F, with the usual sum and the product which results by applying the rule $xa = \sigma(a)x$ for any $a \in F$.

$F[x;\sigma]$ is a left and right Euclidean domain, so every left ideal and every right ideal is principal and any set of elements in $F[x;\sigma]$ has a greatest common right divisor $(-)_r$ and a least common left multiple $[-]_\ell$. If σ has order μ as an automorphism and K is its fixed field, then the center of $F[x;\sigma]$ is $K[x^\mu]$. The center contains $x^n - \lambda$ for any positive multiple n of μ and any $\lambda \in K$. Hence, the n-dimensional F-vector space

$$\mathcal{R} = \frac{F[x;\sigma]}{F[x;\sigma](x^n - \lambda)},$$

which has the canonical F-basis $\{1, x, x^2, \ldots, x^{n-1}\}$, is also a K-algebra and a principal left ideal ring, whose left ideals have the form $\mathcal{R}g$ where g is a right divisor of $x^n - \lambda$.

Definition 4. A *skew λ-constacyclic code* (over F, with respect to σ, of length n, generated by g) is the left ideal of $\mathcal{R}$ generated by g.

Skew λ-constacyclic codes are left ideals and therefore closed under the left multiplication by x, which, through the canonical basis, corresponds to the map

$$(a_0, a_1, \ldots, a_{n-2}, a_{n-1}) \mapsto (\lambda\sigma(a_{n-1}), \sigma(a_0), \sigma(a_1), \ldots \sigma(a_{n-2})),$$

hence their name. The Hamming weight of any element in $\mathcal{R}$ is its number of nonzero entries in its coefficients (with respect to the canonical basis). By suitably choosing g, a prescribed minimum Hamming distance for these codes (that is, the minimum Hamming distance between two distinct codewords) can be guaranteed. Skew BCH constacyclic codes, which are a skew and constacyclic version of the well-known (cyclic) BCH codes, provide a way to do so.

Skew BCH constacyclic codes

If F admits a field extension L over F of degree $s = n/\mu$ such that $\theta : L \to L$ is a field automorphism whose restriction to F is σ and whose fixed field is K, then $F[x;\sigma]$ is a subring of $L[x;\theta]$.

Definition 5. The *θ-conjugate* of $a \in L$ by a nonzero $b \in L$, denoted by a^b, is $b^{-1}a\theta(b)$.

Definition 6. The *i-th truncated norm* of $a \in L$ with respect to θ, denoted by $N_i^\theta(a)$, is 1 for $i = 0$ and $a\theta(a)\theta^2(a)\ldots\theta^{i-1}(a)$ for $i \in \mathbb{Z}^+$.

If $u \in L$ is such that $N_n^\theta(u) = \lambda$ (which corresponds to the norm with respect to the field extension L/K of u being λ), then there are many elements $\alpha \in L$ such that $\left\{\theta^i(\alpha)N_i^\theta(u) \mid 0 \le i \le n-1\right\}$ is a K-basis for L. Then, and as a result of the identity $u^{\theta^i(\alpha)N_i^\theta(u)} = \theta^i(u^\alpha)$, $x^n - \lambda$ can be decomposed as

$$x^n - \lambda = [x - u^{\theta^i(\alpha)N_i^\theta(u)} \mid 0 \le i \le n-1]_\ell = [x - \theta^i(u^\alpha) \mid 0 \le i \le n-1]_\ell,$$

so by choosing a subset of these elements we get generators for skew constacyclic codes. Skew BCH (λ-constacyclic) codes are the ones with the following structure:

Definition 7 ([1, Definition 7])**.** Let $2 \le \delta \le \nu$ and $0 \le r \le n-1$. Then, for

$$g = [x - \theta^{i+j\mu}(u^\alpha) \mid r \le i \le r+\delta-2, 0 \le j \le s-1]_\ell \in F[x;\sigma],$$

the code $\mathcal{R}g$ is called a *skew BCH λ-constacyclic code* of designed Hamming distance δ.

Proposition 8 ([1, Proposition 5])**.** *In the above definition, g is indeed an element in $F[x;\sigma]$. The minimum Hamming distance of a skew BCH λ-constacyclic code of designed Hamming distance δ is, indeed, at least δ. The F-dimension of the code is $n - s\delta + s$.*

Theorem 9 ([1, Theorem 2])**.** *If g is as in Definition 7 and*

$$h = [x - \theta^{i+j\mu}(u^\alpha) \mid r + \delta - 1 \le i \le r + \mu - 1, 0 \le j \le s-1]_\ell,$$

for the same δ and r, then $(\mathcal{R}g, \mathcal{R}h)$ is a linear complementary pair of skew BCH λ-constacyclic codes with security parameter at least δ.

Acknowledgements. The first and second authors have been partially supported, through grant PID2023-149565NB-I00, by MICIU/AEI/10.13039/501100011033. The second author

has been partially supported, through grant PRE2020-093254 by the European Social Fund «ESF Investing in your future».

References

[1] F.J. Lobillo, J.M. Muñoz: Linear complementary pairs of skew constacyclic codes. *Des. Codes Cryptogr.* **93**, 1863–1888 (2025).

[2] X.T. Ngo, S. Bhasin, J.L. Danger, S. Guilley, Z. Najm: *Linear complementary dual code improvement to strengthen encoded circuit against hardware Trojan horses*. IEEE International Symposium on Hardware Oriented Security and Trust (HOST). 82–87 (2015).

Geometric approach to the Modular Isomorphism Problem

L. Margolis[◇*], T. Sakurai[†]

[◇] *Speaker at EACA 2026*

[*] *Departamento de Matemáticas, Universidad Autónoma de Madrid*

[†] *Department of Mathematics and Informatics, Graduate School of Science, Chiba University*

leo.margolis@uam.es, tsakurai@math.s.chiba-u.ac.jp

Abstract. We present an algorithmic approach which uses basic algebraic geometry to determine whether two algebras over a ring are isomorphic. We then apply it to show that if R is a commutative ring in which 2 is not invertible, G is a group of order dividing 64 and H some group, then an isomorphism of group rings $RG \cong RH$ implies an isomorphism $G \cong H$ of groups.

Introduction

For a group finite G and a ring R the group ring RG of G over R is formally a free R-module with basis G, i.e. $\{\sum_{g\in G} r_g g \mid r_g \in R\}$, where the multiplication on the basis G equips RG with a ring structure in a natural way:

$$\left(\sum_{g\in G} r_g g\right)\left(\sum_{g\in G} s_g g\right) = \left(\sum_{g\in G}\left(\sum_{h,k\in G,\ hk=g} r_h s_k\right) g\right).$$

Group Rings are a major tool in the study of groups and their representations, but have also been used in other fields, such as coding theory and knot theory.

The problem we focus on here, the Modular Isomorphism Problem, asks whether the isomorphism of two group algebras of finite p-groups over a field of characteristic p implies an isomorphism of the groups. Though some negative solutions have been found [1, 3, 4], these form a rather isolated class and the problem is far from being well understood in general. We present here a new algorithmic idea to approach the problem and implement it practically to obtain new results.

Our approach is a rather naive way of trying to use some basic algebraic geometry to study the isomorphism of algebras. To explain it, let Γ and Λ be free R-algebras of finite rank over a nonzero commutative ring R. If we want to decide, whether Γ and Λ are isomorphic, an idea could be to try to see, if a subset of R-linearly independent elements in Λ satisfies the relations between the elements of a basis $\mathcal{B}$ of Γ. Thinking about an isomorphism from Γ to Λ and representing the images of elements in $\mathcal{B}$ as generic elements in the basis of Λ in a matrix M, we obtain a matrix in a polynomial ring over R with n^2 variables, where n is the

J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, V. Sotomayor (eds.): Proceedings of the XIX EACA, pp. 192-194 (2026).
ISBN: 978-84-09-87277-0

R-rank of Γ and Λ. The algebraic relations of the elements of $\mathcal{B}$ can then be formulated as polynomials in these variables and the fact that M comes from an isomorphism, means it is an invertible matrix. In particular, we can fill the variables in M with n^2 elements of R such that the values satisfy the relations of $\mathcal{B}$ and make M into an invertible R-matrix, i.e. the determinant of M is a unit in R. So, Γ and Λ are not isomorphic if and only if the polynomials defined by the relations imply that the determinant, as an element of the polynomial ring, is not a unit. This will be particularly the case, when a power of the determinant det lies in the ideal I generated by the relations, i.e. when det is an element in the radical of I. The adjective *geometric* in the title basically refers to this application of the radical of ideals in polynomial rings.

Though this approach seems rather unpractical on a first look, we show that in the context of the Modular Isomorphism Problem it can be sufficiently simplified to obtain:

Theorem: Let R be a commutative ring in which 2 is not invertible, G be a group of order dividing 64 and H a group. If the group rings of G and H over R are isomorphic as R-algebras, then $G \cong H$.

This is not the first algorithm practically implemented to study the Modular Isomorphism Problem. In fact, it is the third after [5] and [2]. The advantage in our approach is that it can detect the non-isomorphism of algebras over all fields of characteristic p at once, while the earlier algorithms were only confirming this over a fixed field, usually the prime field. Admittedly though, our algorithm can not detect, if two algebras are in fact isomorphic. We remark that groups of order 64 were also studied in previous approaches, but these took place only over the prime field.

We will present the basic idea of our algorithm, the tools we use for the implementation, but also some of its limits and cases which we would like to deal with in the same way, but are unable so far.

Acknowledgements. The first author has been partially supported by Ministerio de Ciencia, Innovación y Universidades.

References

[1] C. Bagiński, K. Zabielski: The modular isomorphism problem — the alternative perspective on counterexamples. *J. Pure Appl. Algebra* **229**(1), 107826 (2025).

[2] B. Eick: Computing automorphism groups and testing isomorphisms for modular group algebras. *J. Algebra* **320**(11), 3895–3910 (2008).

[3] D. García-Lucas, L. Margolis, Á. del Río: Non-isomorphic 2-groups with isomorphic modular group algebras. *J. Reine Angew. Math.* **783**, 269–274 (2022).

[4] L. Margolis, T. Sakurai: Identification of non-isomorphic 2-groups with dihedral central quotient and isomorphic modular group algebras. *Rev. Mat. Iberoam.* **41**(5), 1973–2002 (2025).

[5] M. Wursthorn: Isomorphisms of modular group algebras: an algorithm and its application to groups of order 2^6. *J. Symbolic Comput.* **15**(2), 211–227 (1993).

ISOMORPHISMS OF LATTICES OF HYPERINVARIANT AND CHARACTERISTIC SUBSPACES

D. Mingueza*, M.E. Montoro◇†, A. Roca‡

◇ *Speaker at EACA 2026*

* *Nestlé Spain*

† *Universitat de Barcelona*

‡ *Universitat Politècnica de València*

david.mingueza@outlook.es, eula.montoro@ub.edu, aroca@mat.upv.es

Abstract. Given two nilpotent endomorphisms over a finite dimensional space, we characterize when their lattices of hyperinvariant subspaces are isomorphic. The same problem is analyzed for the lattices of characteristic subspaces. The study of the lattices of hyperinvariant and characteristic subspaces of an endomorphism over a finite dimensional space can be reduced to the nilpotent case when the endomorphism has a Jordan-Chevalley decomposition; for example, it occurs when the underlying field is perfect.

INTRODUCTION

Let A be an endomorphism over a finite dimensional vector space over a field $\mathbb{F}$. An A-invariant subspace is *hyperinvariant (characteristic)* if it is T-invariant for all of the matrices T (non singular matrices T) commuting with A. We denote by $\mathrm{Hinv}(A)$ ($\mathrm{Chinv}(A)$) the lattice of hyperinvariant (characteristic) subspaces. Obviously, $\mathrm{Hinv}(A) \subseteq \mathrm{Chinv}(A)$. Moreover, $\mathrm{Hinv}(A) = \mathrm{Chinv}(A)$ but for $\mathbb{F} = GF(2)$, where they can be different ([1]).

The study of the lattices of hyperinvariant and characteristic subspaces of an endomorphism over finite dimensional spaces can be reduced to the nilpotent case when the endomorphism has a Jordan-Chevalley decomposition. For example, it occurs when the underlying field is perfect, in particular over the field of complex numbers (see [5]).

From now on we assume that the endomorphism is represented by a nilpotent Jordan matrix J, therefore, we assume that $\mathbb{F}$ allows a Jordan-Chevalley decomposition.

In this work we present a characterization of isomorphic hyperinvariant lattices, and analyze the main elements that allow us to obtain the result. The next step is to explore to what an extent the same type of elements will be useful to study the characteristic case.

J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, V. Sotomayor (eds.): Proceedings of the XIX EACA, pp. 195-199 (2026).
ISBN: 978-84-09-87277-0

Isomorphisms of lattices of hyperinvariant subspaces

First of all we represent a lattice of hyperinvariant subspaces as a lattice of tuples of integers ([2]). Let $J \in \mathbb{F}^{n\times n}$ be a nilpotent Jordan matrix with Segre characteristic $\alpha = (\alpha_1, \dots, \alpha_m)$, $\alpha_1 \geq \cdots \geq \alpha_m$, $m = \dim\ker(J)$. Fixed a Jordan basis for J, let $u_1, \dots, u_m$ be the generators of the Jordan chains $u_j, Ju_j, \dots, J^{\alpha_j - 1}u_j$, $1 \leq j \leq m$. Given a partition $(k_1, \dots, k_m)$, $0 \leq k_j \leq \alpha_j$, let

$$V(k_1, \dots, k_m) = V^1_{k_1} \oplus \cdots \oplus V^m_{k_m},$$
$$V^j_{k_j} = \text{span}\{J^{\alpha_j - k_j}u_j, \dots, J^{\alpha_j - 1}u_j\}, 1 \leq j \leq m \ \ (V^j_0 = 0).$$

Theorem 1. ([3]) *The subspaces in* $\text{Hinv}(J)$ *are of the form* $V = V(k_1, \dots, k_m)$*, where*

$$k_1 \geq \cdots \geq k_m \geq 0,$$
$$\alpha_1 - k_1 \geq \cdots \geq \alpha_m - k_m \geq 0.$$

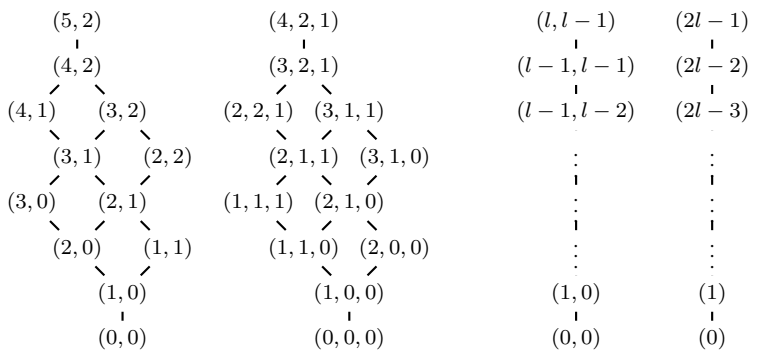
This result allows us to identify the hyperinvariant subpace V with the tuple $(k_1, \dots, k_m)$.

The main result in this section is the next one. It can be found in [6] (stated for $\mathbb{F} = \mathbb{C}$).

Theorem 2. ([6, Theorem 5.13]) *Let* $A, B \in \mathbb{C}^{n\times n}$ *be nilpotent matrices. Let* $\alpha = (\alpha_1, \dots, \alpha_r)$ *and* $\beta = (\beta_1, \dots \beta_s)$ *be the reduced Segre characteristic of* A *and* B*, respectively. Then,* $\text{Hinv}(A) \simeq \text{Hinv}(B)$ *if and only if one of the following conditions are satisfied:*

(i) $\alpha = (5, 2)$ *and* $\beta = (4, 2, 1)$ *or vice-versa.*
(ii) $\alpha = (l, l-1)$ *and* $\beta = (2l-1)$ *for some* $l \geq 2$ *or vice-versa.*
(iii) $\alpha = \beta$.

The proof is gradual: a) $r = 1$; b) $r = 2, s \geq 3$; c) r=s=2; d) r=s=3; e) r=s; f) general case.



Hyperlattices: (5,2) (4,2,1) (l, l-1) (2l-1)

To do it, we have introduced some important notions in the lattice and have analyzed its properties. These are the notion of a *son* of a hyperinvariant subspace, a *chain* of hyperinvariant subspaces, a *special chain ending at zero* and the possible types of it, and a *riding chain* ([6]). We include here these concepts.

Definition 3. Given $u = (u_1, \ldots, u_r) \in V(\alpha_1, \ldots, \alpha_r)$, we say that $v = (v_1, \ldots, v_r) \in V(\alpha_1, \ldots, \alpha_r)$ is a *son* of u if there exists $j \in \{1, \ldots, r\}$ such that $v_i = u_i$ for $i \in \{1, \ldots, r\} \setminus \{j\}$, $v_j = u_j - 1$.

We have given a characterization of a son. Among the chains, are important the so called special chains and riding special chains.

Definition 4. Given $V(\alpha_1, \ldots, \alpha_r)$, a *chain* C of length t from w_1 to w_t is a sequence of hypertuples $w_1, \ldots, w_t \in V(\alpha_1, \ldots, \alpha_r)$ such that $w_{i+1} \in \mathrm{Son}(w_i),\ i = 1, \ldots, t-1$. We will write the chain C as $w_1 - \cdots - w_t$.

Definition 5. A chain $C : w_1 - w_2 - \cdots - w_t$ in $V(\alpha_1, \ldots, \alpha_r)$ is called *special* if it is of maximal length satisfying the property that $Son(w_i) = \{w_{i+1}\},\ i = 1, \ldots, t-1$.

We are interested in special chains ending at zero; there are only three types of them.

Theorem 6. *In the hyperlattice $V(\alpha_1, \ldots, \alpha_r)$, $r \geq 2$, there exist at most two of the three possible types of special chains ending at zero, C_1, C_2 and C_3, of lengths $r+1, \alpha_1 - \alpha_2 + 1$ and $2(\alpha_1 - \alpha_3)$, respectively, defined as follows:*

C_1	C_2 (*if* $\alpha_1 - \alpha_2 > 1$)	C_3 (*if* $\alpha_1 - \alpha_2 = 1$)
$(1, 1, \ldots, 1, 1)$	$(\alpha_1 - \alpha_2, 0, \ldots, 0)$	$(\alpha_1 - \alpha_3, \alpha_2 - \alpha_3, 0, \ldots, 0)$
$\vert$	$\vert$	$\vert$
$(1, 1, \ldots, 1, 0)$	$(\alpha_1 - \alpha_2 - 1, 0, \ldots, 0)$	$(\alpha_1 - \alpha_3 - 1,\ \alpha_2 - \alpha_3, 0, \ldots, 0)$
$\vert$	$\vert$	$\vert$
		$(\alpha_1 - \alpha_3 - 1, \alpha_2 - \alpha_3 - 1, 0, \ldots, 0)$
$\vdots$	$\vdots$	$\vdots$
$\vert$	$\vert$	$\vert$
$(1, 0, \ldots, 0, 0)$	$(1, 0, \ldots, 0)$	$(1, 0, \ldots, 0)$
$\vert$	$\vert$	$\vert$
$(0, 0, \ldots, 0, 0)$	$(0, 0, \ldots, 0)$	$(0, 0, \ldots, 0)$

Definition 7. Given $p \in \{1, 2, 3\}$, a chain $RC_p : w_1 - w_2 - \cdots - w_l$ *rides* on a special chain C_p if it is of maximal length satisfying that $\exists j \in \{1, \ldots, l-1\}$ such that $\mathrm{Son}(w_i) = \{w_{i+1}\}$ for $1 \leq i \leq j$, and for $j+1 \leq i \leq l-1$, $\mathrm{Son}(w_i) = \{w_{i+1}, w'_{i+1}\}$ with $w'_{i+1} \in C_p$, and $\mathrm{Son}(w_l) = \{w'_{l+1}\}$ with $w'_{l+1} \in C_p$.

We must say that isomorphisms of hyperinvariant lattices were studied in [8], and although the statement of the final result was correct, the analysis was incomplete and several partial result were defective. Based on the ideas of this paper, we completed the analysis, providing a proof of a characterization of isomorphic hyperinvariant subspaces (see [6]).

Isomorphisms of lattices of characteristic subspaces

The target of the second part of the work is to study isomorphisms of lattices of characteristic subspaces when $\mathbb{F} = GF(2)$. We see Chinv(J) = Hinv$(J) \cup$ (Chinv$(J) \setminus$ Hinv(J)). A theorem by Shoda asserts that there exist subspaces in Chinv$(J) \setminus$ Hinv(J) if and only if there are at least two Jordan blocks of unique sizes α_i, α_j such that $|\alpha_i - \alpha_j| > 1$ ([7]).

First of all let us present the description of characteristic subspaces obtained in [4].

Definition 8. A *chartuple* is a tuple of positive integers $b = (b_{i_1}, \ldots, b_{i_t})$, $t \geq 2$, where $i_1, \ldots, i_t$ correspond to α_{i_j} appearing just once in the Segre characteristic of J, satisfying

$$b_{i_1} > b_{i_2} > \cdots > b_{i_t} > 0,$$
$$\alpha_{i_1} - b_{i_1} > \alpha_{i_2} - b_{i_2} > \cdots > \alpha_{i_t} - b_{i_t} \geq 0.$$

Given a chartuple $b = (b_{i_1}, \ldots, b_{i_t})$, we define $z_1, \ldots, z_t$ as $z_j = J^{\alpha_{i_j} - b_{i_j}} u_{i_j}$, $\quad 1 \leq j \leq t$. A subspace Z is a *minext subspace* associated to $(b_{i_1}, \ldots, b_{i_t})$ if every $z \in Z$ is of the form

(i) $z = z_{i_1} + \cdots + z_{i_p}, \quad p \leq t, \quad 1 \leq i_1 < i_2 < \ldots < i_p \leq i_t,$
(ii) $z_j \notin Z, \quad 1 \leq j \leq t,$
(iii) each z_j appears as a summand of some $z \in Z$, i.e.

$$\dim(span\{z_1, \ldots, \hat{z_j}, \ldots, z_t\} + Z) = t, \quad 1 \leq j \leq t.$$

A hyperinvariant subspace Y is a *hyperinvariant subspace* associated to $b = (b_{i_1}, \ldots, b_{i_t})$ if it is of the form:

$$Y = V(k_1, \ldots, k_{i_1 - 1}, b_{i_1} - 1, k_{i_1+1}, \ldots, k_{i_t - 1}, b_{i_t} - 1, k_{i_t+1}, \ldots, k_m),$$

and the following subspace is also hyperinvariant:

$$V(k_1, \ldots, k_{i_1 - 1}, b_{i_1}, k_{i_1+1}, \ldots, k_{i_2 - 1}, b_{i_2}, k_{i_2+1}, \ldots, k_{i_t - 1}, b_{i_t}, k_{i_t+1}, \ldots, k_m).$$

Theorem 9. ([4]) *Let $J \in M_n(GF(2))$ be a nilpotent Jordan matrix and $\alpha = (\alpha_1, \ldots, \alpha_m)$ its Segre characteristic. Then, $X \in$ Chinv$(J) \setminus$ Hinv(J) if and only if $X = Y \oplus Z$ where Y and Z are a hyperinvariant and a minext subspaces associated to a given char-tuple, respectively.*

Our approach to study the problem is the same as in the previous case. We have characterized when a characteristic subspace is the son of another characteristic one. We try to extend the notions of special chains ending at zero and riding chains introduced in the study of isomorphisms of lattices of hyperinvariant subspaces to lattices of characteristic subspaces, in order to study its behavior face to isomorphic transformations.

Acknowledgements. The second and third authors have been partially supported by grant PID2019-104047GB-I00 and by grant PID2021-124827NB-I00 funded by MCIN/AEI/10.13039/501100011033 and by «ERDF A way of making Europe» by the European Union.

References

[1] P. Astuti, H.K. Wimmer: Characteristic and hyperinvariant subspaces over the field $GF(2)$. *Linear Algebra Appl.* **438**(4), 1551–1563 (2013).

[2] P.A. Fillmore, D.A. Herrero, W.E. Longstaff: The hyperinvariant subspace lattice of a linear transformation. *Linear Algebra Appl.* **17**, 125–132 (1977).

[3] I. Gohberg, P. Lancaster, L. Rodman: *Invariant Subspaces of Matrices with Applications*. SIAM (1986).

[4] D. Mingueza, M.E. Montoro, J.R. Pacha: Description of the characteristic non-hyperinvariant subspaces over the field GF(2). *Linear Algebra Appl.* **439**, 3734–3745 (2013).

[5] D. Mingueza, M.E. Montoro, A. Roca: The lattice of characteristic subspaces of an endomorphism with Jordan-Chevalley decomposition. *Linear Algebra Appl.* **558**, 63–73 (2018).

[6] D. Mingueza, M.E. Montoro, A. Roca: Isomorphisms between lattices of hyperinvariant subspaces. *Linear Algebra Appl.* **703**, 395–422 (2024).

[7] K. Shoda: Über die charakteristischen Untergruppen einer endlichen Abelschen Gruppe. *Math. Z.* **31**, 611–624 (1930).

[8] P.Y. Wu: Which Linear Transformations Have Isomorphic Hyperinvariant Subspace Lattices? *Linear Algebra Appl.* **169**, 163–178 (1992).

Algoritmos para calcular los strands de la resolución de Taylor de ideales monomiales libres de cuadrados

P. Munarriz-Senosiain[◇*], E. Sáenz-de-Cabezón[*]

[◇] *Conferenciante en el EACA 2026*

[*] *Universidad de La Rioja*

pablo.munarriz@unirioja.es, eduardo.saenz-de-cabezon@unirioja.es

Resumen. We describe iterative algorithms for the efficient computation of the strands of the Taylor resolution of a squarefree monomial ideal.

Introducción

Sea $I \subseteq \mathbf{k}[x_1, \ldots, x_r]$ un ideal monomial y $G(I) = \{m_1, \ldots, m_n\}$ su conjunto generador monomial minimal. Sea $\mathcal{F}$ una resolución (no necesariamente mínima) libre multigraduada de I. Dado un multigrado $\mu \in \mathbb{N}^r$, definimos el μ-strand de $\mathcal{F}$ como el conjunto de submódulos de los módulos de $\mathcal{F}$ generados en multigrado μ, y la restricción de los morfismos de $\mathcal{F}$ a estos submódulos.

En el caso de los ideales libres de cuadrados, el $\mathbb{1}$-strand es particularmente importante (notamos $\mathbb{1} = (1 \cdots 1)$), ya que, gracias a la fórmula de Hochster [2], su cálculo permite obtener la homología de complejos simpliciales. En [1], este hecho se usó, unido a los árboles de Mayer-Vietoris, para el cálculo eficiente de dichos grupos de homología en el caso en el que el número de caras maximales del complejo es pequeño en relación al número de vértices. En este trabajo proponemos un acercamiento a este problema basado en el $\mathbb{1}$-strand de la resolución de Taylor [3], describiendo algoritmos para calcularlo de forma eficiente.

Obsérvese lo siguiente: Sean $I \subseteq \mathbf{k}[x_1, \ldots, x_r]$ un ideal monomial libre de cuadrados, $G(I)$ su conjunto generador monomial minimal y $\mu \in \{0,1\}^r$ un multigrado cualquiera. Sin pérdida de generalidad, podemos suponer que $\mu = (1 \cdots 1\, 0 \cdots 0)$, con r' unos. Consideremos el ideal monomial libre de cuadrados $I' \subseteq \mathbf{k}[x_1, \ldots, x_{r'}]$ generado por los monomios de $G(I)$ que no son múltiplos de ningún x_i, con $i > r'$. Entonces, resulta que el μ-strand de la resolución de Taylor de I es el $\mathbb{1}$-strand de la resolución de Taylor de I'. En definitiva, los algoritmos que proponemos sirven para obtener todos los strands de la resolución de Taylor de cualquier ideal monomial libre de cuadrados.

El $\mathbb{1}$-strand de la resolución de Taylor

En lo que sigue, siempre se trabajará con ideales monomiales libres de cuadrados, y cuando se mencione un conjunto de monomios, estos monomios se asumirán libres de

J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, V. Sotomayor (eds.): Proceedings of the XIX EACA, pp. 200-205 (2026).
ISBN: 978-84-09-87277-0

cuadrados. Además, consideraremos que el cuerpo **k** sobre el que construimos el anillo de polinomios tiene característica 2.

Definición 1. Un conjunto de monomios σ es $\mathbb{1}$-*strand* si $\operatorname{lcm}(\sigma) = \mathbf{x}^{\mathbb{1}}$. Es decir, si cada variable del anillo aparece al menos en un monomio de σ.

Observación 2. Si $\sigma_1 \subseteq \sigma_2$, se tiene que si σ_1 es $\mathbb{1}$-strand, entonces σ_2 también es $\mathbb{1}$-strand. Equivalentemente, si σ_2 no es $\mathbb{1}$ strand, entonces σ_1 tampoco lo es.

Definición 3. Para cada $k \in \mathbb{N} \cup \{0\}$, definimos $S_k = \{\sigma \subseteq G(I) \mid \sigma \text{ es } \mathbb{1}\text{-strand y } |\sigma| = k\}$.

Las matrices M_k del $\mathbb{1}$-strand de la resolución de Taylor de I sobre $\mathbb{Z}_2$ son las asociadas a los homomorfismos de la resolución de Taylor de I restringidos a los módulos libres generados por S_k. Para cada $k \in \mathbb{N}$, la matriz M_k viene dada por:

- las columnas representan los conjuntos de S_k,
- las filas representan los conjuntos de S_{k-1},
- la posición ij vale 1 si el representante de la fila i es subconjunto del representante de la columna j, y 0 en caso contrario.

Ejemplo 4. Consideremos el ideal $I = \langle xy, xt, yz, yt, zt\rangle$ sobre el anillo $\mathbf{k}[x, y, z, t]$. Es rutinario comprobar que:

$$
\begin{aligned}
S_2 &= \{xy, zt\}, \{xt, yz\}\},\\
S_3 &= \{\{xy, xt, yz\}, \{xy, xt, zt\}, \{xy, yz, yt\}, \{xy, yz, zt\}, \{xy, yt, zt\}, \{xt, yz, yt\},\\
&\quad \{xt, yz, zt\}, \{xt, yt, zt\}\},\\
S_4 &= \{\{xy, xt, yz, yt\}, \{xy, xt, yz, zt\}, \{xy, xt, yt, zt\}, \{xy, yz, yt, zt\}, \{xt, yz, yt, zt\}\},\\
S_5 &= \{G(I)\}, \quad S_0 = S_1 = S_k = \emptyset, \text{ para cada } k > 5.
\end{aligned}
$$

Así, las únicas matrices no vacías del $\mathbb{1}$-strand de la resolución de Taylor de I sobre $\mathbb{Z}_2$ son:

$$
M_3 = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}, \quad M_4 = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix},
$$

$$
M_5 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \end{pmatrix}.
$$

El objetivo de este trabajo es diseñar algoritmos iterativos que, dado el conjunto generador minimal de un ideal monomial libre de cuadrados, computen las matrices M_k.

Representación binaria del problema

Codificamos un monomio como el vector de sus exponentes en $\mathbb{Z}_2^r$. Para codificar conjuntos de monomios almacenamos las codificaciones de los monomios como filas de una matriz en $\mathbb{Z}_2$. Así, un conjunto de monomios es $\mathbb{1}$-strand si y solo si la matriz asociada al conjunto no tiene ninguna columna nula.

Ejemplo 5. Sea $I = \langle xy, xt, yz, yt, zt\rangle \subseteq \mathbf{k}[x, y, z, t]$ y sea $\sigma = \{xy, xt\}$. Las matrices A y B asociadas a $G(I)$ y σ respectivamente, son

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

Vemos que $G(I)$ es $\mathbb{1}$-strand porque todas las columnas de A son no nulas, pero σ no es $\mathbb{1}$-strand porque B tiene la tercera columna (correspondiente a la variable z) vacía.

Para codificar un subconjunto $\sigma \subseteq G(I)$ usaremos el vector $v_\sigma \in \mathbb{Z}_2^n$ que indica la pertenencia de cada monomio de $G(I)$ a σ. Dada la matriz que codifica a $G(I)$ como conjunto de monomios y el vector $v_\sigma \subseteq G(I)$, para obtener la matriz que codifica a σ basta con quedarse con las filas de la matriz de $G(I)$ determinadas por v_σ. Además, dados los vectores v_{σ_1} y v_{σ_2} asociados a dos subconjuntos σ_1 y σ_2 de $G(I)$, $\sigma_1 \subseteq \sigma_2$ si y solo si $v_{\sigma_1} \leq v_{\sigma_2}$ componente a componente.

Ejemplo 6. Sea $I = \langle xy, xt, yz, yt, zt\rangle \subseteq \mathbf{k}[x, y, z, t]$. Consideremos los subconjuntos de $G(I)$ $\sigma_1 = \{xy, xt\}$, $\sigma_2 = \{xt, yt\}$ y $\sigma_3 = \{xy, xt, zt\}$. Tenemos que $v_{\sigma_1} = (1, 1, 0, 0, 0)$, $v_{\sigma_2} = (0, 1, 0, 1, 0)$ y $v_{\sigma_3} = (1, 1, 0, 0, 1)$, vemos que $\sigma_1 \subseteq \sigma_3$ y que no hay ninguna otra relación de inclusión entre los subconjuntos considerados.

Usando esta representación del problema, podemos obtener las matrices M_k a partir de la matriz asociada a $G(I)$ como conjunto de monomios. Así, la abstracción del problema sería la siguiente.

Definición 7. Una matriz sobre $\mathbb{Z}_2$ es $\mathbb{1}$*-strand* si no tiene columnas nulas.

Definición 8. Dada una matriz A sobre $\mathbb{Z}_2$ con n filas, una cadena C de n bits es $\mathbb{1}$*-strand* si la submatriz de A formada por las filas determinadas por los unos de C es $\mathbb{1}$-strand.

Definición 9. Sean C_1 y C_2 cadenas de n bits. Decimos que C_1 es *descendiente* de C_2, denotado $C_1 \preceq C_2$, si cada componente de C_1 es menor o igual que la respectiva componente de C_2. En tal caso, también diremos que C_2 es *ascendiente* de C_1.

Observación 10 (ver Observación 2)**.** Si una cadena es $\mathbb{1}$-strand, entonces todas sus ascendientes también lo son; y si no es $\mathbb{1}$-strand, sus descendientes tampoco lo son.

Sea una matriz sobre $\mathbb{Z}_2$ de tamaño $n \times r$. Abusando de notación, consideraremos, para cada $k \in \mathbb{N} \cup \{0\}$, los conjuntos S_k formados por las cadenas de n bits que sean $\mathbb{1}$-strand y tengan k unos. Finalmente, para cada $k \in \mathbb{N}$, consideramos la matriz M_k definida como sigue:

- las columnas representan las cadenas de S_k,
- las filas representan las cadenas de S_{k-1},
- la posición ij vale 1 si la representante de la fila i es descendiente de la representante de la columna j, y 0 en caso contrario.

Diagrama y reglas para recorrerlo

De cara a construir algoritmos iterativos tratando de minimizar los cálculos innecesarios o redundantes, nos centraremos en la manera en la que recorreremos las cadenas de n bits. El objetivo es aprovechar la Observación 10, para ello, establecemos un orden adecuado en las cadenas. Además, queremos que recorrer las cadenas sea eficiente tanto en cuanto a la cantidad de operaciones necesarias como en la cantidad de memoria requerida.

Representaremos todas las posibles cadenas en un diagrama análogo al de la Figura 1. Separamos por filas las cadenas en función del número de unos que tienen. Cada fila la ordenamos de izquierda a derecha según el orden lexicográfico.

El orden en el que recorreremos las cadenas viene determinado por las siguientes reglas:

1. Empezamos por la cadena formada por n unos.
2. Si estamos en una cadena que acaba en 1, para pasar a la siguiente ponemos a 0 el primer 1 después del último 0.
3. Si estamos en una cadena que acaba en 0, para pasar a la siguiente tenemos tres posibilidades:
    - Si el penúltimo bit es 0, lo ponemos a 1.
    - Si el penúltimo bit es 1, ponemos los dos últimos 0s a 1, y el siguiente bit del que era el penúltimo 0 (que acabamos de cambiar a uno) lo ponemos a 0.
    - Si no hay más ceros, hemos terminado.

En la Figura 1 podemos ver el recorrido que seguimos cuando $r = 4$.

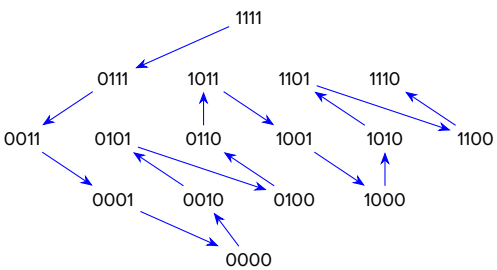


Figura 1. Diagrama y recorrido con 4 generadores.

Sea C una cadena acabada en 1 y C' la siguiente cadena en la fila de C. Se puede probar que todas las cadenas entre C y C' (no incluida) son descendientes de C. Es más, tanto C' como todas las cadenas sucesivas no son descendientes de C. Este hecho, junto con la Observación 10, nos dice que si C no es $\mathbb{1}$-strand, entonces todas las cadenas entre C y C' tampoco son $\mathbb{1}$-strand, por lo que podemos saltar directamente de C a C'. Para ello bastará con poner el último 0 de C a 1 y el siguiente bit a 0.

Coordenadas

Otra forma de representar las cadenas del diagrama es indicando la posición de los ceros de la cadena mediante tuplas que cuentan el número de unos entre cada cero. Es decir, para determinar una cadena de longitud n con k unos necesitaremos una $(n-k)$-tupla que tenga en la i-ésima posición la cantidad de unos que hay entre el $(i-1)$-ésimo y el i-ésimo cero. Por ejemplo, la cadena formada por todo unos la representamos mediante una tupla vacía, la cadena 1101 mediante la 1-tupla (2), y la cadena 0010 mediante la 3-tupla $(0,0,1)$. A estas tuplas les llamamos *coordenadas* de las cadenas. Si bien es cierto que almacenar tuplas puede requerir más memoria que almacenar cadenas, resulta que hay ciertos cálculos para los que es más eficiente usar coordenadas en vez de cadenas.

Conclusión

El objetivo de este trabajo es diseñar algoritmos iterativos para computar eficientemente las matrices del $\mathbb{1}$-strand de la resolución de Taylor sobre $\mathbb{Z}_2$ de ideales monomiales libres de cuadrados. Para ello, traducimos el problema a binario y diseñamos algoritmos a bajo nivel tratando de explotar las propiedades de los objetos que codificamos.

Todos los algoritmos propuestos en este trabajo se basan en una forma concreta de recorrer los subconjuntos del conjunto generador monomial minimal del ideal. La diferencia entre unos y otros algoritmos es la forma en la que representamos estos subconjuntos, la cantidad de información que almacenamos o la forma en la que construimos las matrices.

Debido a que calcular el μ-strand de la resolución de Taylor de un ideal monomial libre de cuadrados se reduce a calcular el $\mathbb{1}$-strand de la resolución de Taylor de otro ideal monomial libre de cuadrados, resulta que los algoritmos propuestos permiten obtener eficientemente todos los strands de la resolución de Taylor de cualquier ideal monomial libre de cuadrados.

Agradecimientos. Este trabajo ha sido parcialmente financiado por el proyecto PID2024-157733NBI00, financiado por MCIN/AEI/10.13039/501100011033/FEDER EU.

Referencias

[1] A.M. Bigatti, J. Heras, E. Sáenz-de Cabezón: *Monomial resolutions for efficient computation of simplicial homology*. Proceedings of ISSAC 2019, 50–57. ACM (2019).

[2] M. Hochster: *Cohen-Macaulay rings, combinatorics, and simplicial complexes*. Ring Theory II. B.R. McDonald, R. Morris (eds.), 171–223. Marcel Dekker (1977).

[3] D.K. Taylor: *Ideals generated by monomials in an r-sequence*. PhD thesis, University of Chicago (1966).

Toward a symbolic framework for locus computation: Insights from Maple-based algebraic analysis

T. Recio*, R. Rubio◇*, M. Pilar Vélez*
◇ *Speaker at EACA 2026*
* *Universidad Antonio de Nebrija*
trecio@nebrija.es, mrubio@nebrija.es, pvelez@nebrija.es

Abstract. Current implementations of locus calculations in GeoGebra Discovery rely on numerical equations that limit the mathematical versatility of the LocusEquation command. While the system integrates advanced symbolic reasoning tools, its locus result still generates polynomials with numerical coefficients, forcing users to infer the exact algebraic structure through visual inspection or human intuition. In this work, using non-trivial examples and Maple as a reference system, we illustrate the shortcomings of numerical locus computation and highlight the need for incorporating fully symbolic algorithms into dynamic geometry environments. We argue for the integration of symbolic locus computation directly into GeoGebra Discovery, enabling more rigorous, automated verification and strengthening technology-supported mathematical understanding.

Introduction

Locus computation has long been recognized as a characteristic and defining feature of Dynamic Geometry (DG) software [2]. As stated by X.-S. Gao (1999), «*There is a wide consensus among DG developers to consider locus computation as one of the five basic properties in the DG paradigm (together with dynamic transformation, measurement, free dragging and animation)*» [3]. This situates locus construction not as an auxiliary tool, but as a cornerstone capability that shapes the expressive power of DG systems.

The study of geometric loci within dynamic geometry environments has also gained increasing relevance in mathematics education, particularly in contexts where technology supports and amplifies students' reasoning processes. GeoGebra Discovery, an experimental branch of GeoGebra enriched with automated reasoning tools, offers valuable opportunities for inquiry-based exploration. However, its *LocusEquation* command still relies on numerical equations, requiring users to infer the underlying symbolic structure of the locus and verify it through additional tools. This work examines these limitations and argues for the integration of symbolic computation methods to strengthen both the mathematical rigor and the pedagogical impact of dynamic geometry systems.

J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, V. Sotomayor (eds.): Proceedings of the XIX EACA, pp. 206-210 (2026).
ISBN: 978-84-09-87277-0

Numerical locus computation in GeoGebra discovery

Although GeoGebra Discovery incorporates symbolic protocols for automated reasoning, its locus engine does not yet fully leverage these capabilities. The numerical workflow generates equations sensitive to coordinate choices, complicating the identification of exact curves and making it difficult to discern whether the calculated loci correspond to algebraic varieties.

Roughly, it proceeds by performing an elimination algorithm on the ideal generated by the equations describing the construction steps, plus the equation describing the defining constraint. Currently, in GeoGebra, the construction equations are introduced in the elimination algorithm by considering the numerical coordinates of the free points in the construction. In summary, the output is an exact, symbolic equation but for a specific, numerical locus, the one corresponding to the initial points or data in the figure, not a generic, parametric locus that presents the locus equation for all possible positions of the involved construction, as it would not be possible to display this generic output.

Yet, it could have been possible for GeoGebra to consider an alternative approach, first introducing the equations of the construction and of the imposed condition, assigning symbolic coordinates to the involved points, and then proceeding to the elimination step to obtain a generic locus. A locus that could be graphically displayed by substituting the symbolic coordinates by the numerical values of the concrete points shown in the graphics view window. We consider this current approach of GeoGebra to locus computation to be specially unexpected, since GeoGebra's *Prove* or *Relation* commands already proceed assigning symbolic variables to the free points coordinates of the involved construction, to obtain mathematically correct and general answers to the addressed questions about geometric properties holding on the figure.

Another argument to favor the relevance of the symbolic approach to locus computation is the consideration of locus computation as a potential instrument for the automated discovery of geometric statements (see [1] for a more detailed description), by considering the locus condition as an additional hypothesis to be added to the construction steps, and the locus output as the corresponding thesis.

Maple-based symbolic approaches and future perspectives

To demonstrate the advantages of symbolic methods, we analyzed a non-trivial geometric configuration using Maple, obtaining an exact algebraic description of the locus through elimination techniques and precise coefficient manipulation. The resulting curve reveals structural features that cannot be derived solely from the numerical information provided by GeoGebra Discovery.

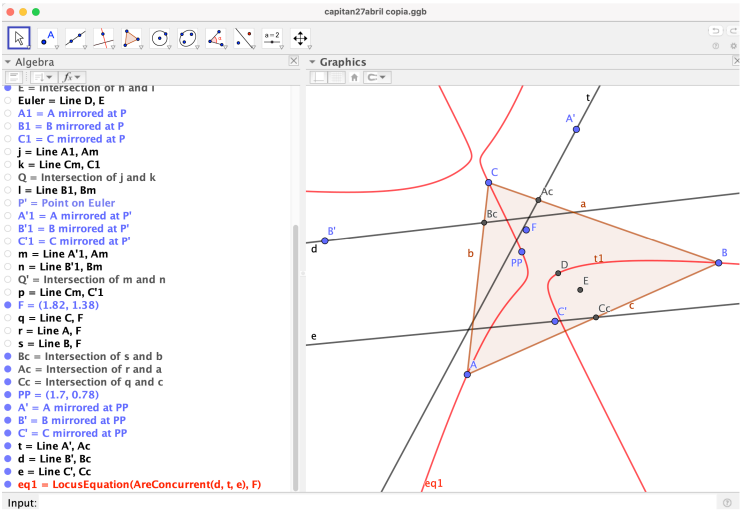
In our current work, we aim to formulate and to deal with some computer algebra questions involved in the possible improvement of loci calculation. This will be achieved by exploring some challenging situations, highlighting the difficulties that arise in such cases when

attempting to develop a purely symbolic approach, and using Maple as a computational tool to illustrate the possible treatment of such problems.

A summary of the questions we intend to address could be the following:

1. How to deal with purely symbolic locus, i.e. with locus defined in the context of geometric constructions with arbitrary (parametric) coordinates, and, in this context, how to visualize the output by dealing with the corresponding specialization for numerical values of the coordinates of the basic points of the same construction? Should we first specialize and then compute the locus or, conversely, first compute the generic locus and then specialize? Will both approaches yield the same output?
2. Should we consider, in the *EliminationIdeal* protocol that is usually associated to locus computation, the parameters as variables or as elements of the field of coefficients? Will both approaches yield the same output?

Let us illustrate some of these points with an example from [4], a generalization of a problem proposed by D. Nguyen in 2025 and disseminated through the blog of García Capitán who leads a highly active international community of enthusiasts of elementary geometry problems, with a broad online presence spanning Facebook groups, blogs, online journals, and a Telegram channel. The construction is as follows: Given a triangle ABC, we consider a general point F and the feet of the lines AF, BF, CF, (Ac, Bc, Cc, respectively). Next, we consider another arbitrary point PP and A', the point A mirrored at PP, B' and C' (likewise). Then we define lines $A'Ac$, $B'Bc$ and $C'Cc$. And we wonder where to place F in order to obtain the concurrency of the three lines.



The output is the red curve, a cubic one.

If we want to translate this construction to Maple, we can consider $A(0,0)$ and $B(1,0)$ without loss of generality, while keeping C, F and PP as generic points. *Pre* is the ideal of the construction, without the lines $A'Ac$, $B'Bc$, $C'Cc$.

Next, we can prove that C, F and PP are free points in the construction.

```
> EliminationIdeal(Pre,{c1,c2,f1,f2,pp1,pp2});
```

$$\langle 0 \rangle$$

Cond is the ideal of the construction *Pre*, but adding that $A'Ac$, $B'Bc$ and $C'Cc$ are concurrent at the point (x, y):

Finally, we determine the locus of F for which the concurrency occurs, that is, we do the following elimination as a function of the other two free points, C and PP:

```
> EqnLocus:=EliminationIdeal(Cond,{c1,c2,f1,f2,pp1,pp2});
```

We get a cubic in $f1$, $f2$, with coefficients the coordinates of C and PP, multiplied by $c2$. This last factor $c2 = 0$, is a degenerate case, since it means ABC are aligned, not a triangle.

$$\begin{aligned}
&\langle -c2(2c1^3 f2^3 pp2 - 2c1^3 f2^2 pp2^2 - 4c1^2 c2 f1 f2^2 pp2 - 2c1^2 c2 f2^3 pp1 + 6f2^2 pp1pp2 c1^2 c2 \\
&+ 6c1^2 f1 f2^2 pp2^2 - 6c1^2 f2^3 pp1pp2 + 2f1^2 f2pp2c1 c2^2 + 2f1^2 pp2^2 c1 c2^2 + 4f1 f2^2 pp1c1 c2^2 \\
&- 4f1f2pp1pp2c1 c2^2 - 4f2^2 pp1^2 c1 c2^2 - 8f1^2 f2 pp2^2 c1c2 + 4f1 f2^2 pp1pp2c1c2 \\
&+ 4c1c2 f2^3 pp1^2 - 2f1^2 f2pp1 c2^3 - 2f1^2 pp1pp2 c2^3 + 4c2^3 f1f2 pp1^2 + 2c2^2 f1^3 pp2^2 \\
&+ 2f1^2 f2pp1pp2 c2^2 - 4c2^2 f1 f2^2 pp1^2 + c1^2 c2 f2^3 - f2^2 pp2 c1^2 c2 - 2c1 c2^2 f1 f2^2 \\
&- 2f1 pp2^2 c1 c2^2 + 2c1 c2^2 f2^2 pp1 + 2f2pp1pp2c1 c2^2 + 2c1c2f1 f2^2 pp2 + 8c1c2f1f2 pp2^2 \\
&- 2c1c2 f2^3 pp1 - 8c1c2 f2^2 pp1pp2 - 6c1f1 f2^2 pp2^2 + 6c1 f2^3 pp1pp2 + c2^3 f1^2 f2 \\
&+ c2^3 f1^2 pp2 - 2c2^3 f1f2pp1 + 2c2^3 f1pp1pp2 - 2c2^3 f2 pp1^2 - 2c2^2 f1^2 f2pp2 - 4c2^2 f1^2 pp2^2 \\
&+ 2c2^2 f1 f2^2 pp1 + 4c2^2 f2^2 pp1^2 + 4c2 f1^2 f2 pp2^2 - 2c2f1 f2^2 pp1pp2 - 2c2 f2^3 pp1^2 \\
&+ c1c2 f2^3 - c1c2 f2^2 pp2 - 2c1 f2^3 pp2 + 2c1 f2^2 pp2^2 - c2^3 f1pp2 + c2^3 f2pp1 - c2^2 f1 f2^2 \\
&+ 2c2^2 f1f2pp2 + 2c2^2 f1 pp2^2 - c2^2 f2^2 pp1 - 2c2^2 f2pp1pp2 + 2c2f1 f2^2 pp2 - 4c2f1f2 pp2^2 \\
&+ 2c2 f2^2 pp1pp2)\rangle
\end{aligned}$$

Now, for a concrete instance, we give values to $c1$, $c2$, $pp1$, $pp2$ in the above cubic:

```
> Es:=subs(c1=1/3,c2=2,pp1=1/2,pp2=1/3, op(eqnLocus));
```

$$Es := \frac{8}{9} f1^3 - \frac{26}{9} f1 f2^2 + \frac{16}{27} f1 - \frac{4}{27} f1^2 f2 + \frac{40}{27} f1f2 + \frac{430}{243} f2^2 - \frac{25}{81} f2^3 - \frac{8}{9} f2 - \frac{40}{27} f1^2$$

We observe that this equation coincides with the locus obtained if we do first the substitution for these values of $C = \left(\frac{1}{3}, 2\right)$ and $PP = \left(\frac{1}{2}, \frac{1}{3}\right)$ and then the elimination. Similarly, with whatever other values we substitute in the symbolic locus. Can we confirm this is always true (in this example)? Is this always true (in general)?

This illustrates some of the issues involved in our protocol to address the proposed questions.

Acknowledgements. Authors have been partially granted by Comunidad de Madrid, Proyecto IAxEM-CM, PHS-2024/PH-HUM-383.

References

[1] M. Abánades, F. Botana, Z. Kovács, T. Recio, C. Sólyom-Gecse: *Towards the Automatic Discovery of Theorems in GeoGebra*. Mathematical Software – ICMS 2016, Lecture Notes in Computer Science **9725**, 37–42. Springer (2016).

[2] M. Abánades, F. Botana, A. Montes, T. Recio: An algebraic taxonomy for locus computation in dynamic geometry. *Computer-Aided Design* **56**, 22–33 (2014).

[3] X.S. Gao: *Automated geometry diagram construction and engineering geometry*. ADG 1998, Lecture Notes in Artificial Intelligence **1669**, 232–257. Springer (1999).

[4] F. García Capitán: Generalizing problem Nguyen085. `https://garciacapitan.blogspot.com/2025/04/generalizing-problem-nguyen085.html` (2025).

Spohn conditional independence varieties of generic games

J. Sendra-Arranz[◇*], M. Bouyer[†‡], I. Portakal[‡]

[◇] *Speaker at EACA 2026*

[*] *Department of Mathematics, CUNEF Universidad*

[†] *École Polytechnique*

[‡] *Max Planck Institute for Mathematics in the Sciences*

javier.sendraarranz@cunef.edu, matthieu.bouyer@polytechnique.org, mail@irem-portakal.de

Abstract. We further develop the algebraic–geometric foundations of conditional independence (CI) equilibria, a refinement of Nash and dependency equilibria that integrates conditional independence relations from graphical models into strategic reasoning. Extending earlier work on binary games, we analyze the structure of the associated Spohn CI varieties for generic games of arbitrary format. We compute the dimension of the Spohn CI variety for generic games. We show that when non-empty, the set of totally mixed CI equilibria forms a smooth manifold for generic games. For cluster graphical models, we introduce the class of Nash CI varieties, prove their irreducibility, and describe their defining equations, degrees, and conditions for the existence of totally mixed CI equilibria for generic games. This extended abstract is based on the preprint arXiv:2511.11467.

Introduction

Game theory has had a broad impact, particularly through applications in economics, and many advances have arisen from interactions with other areas of mathematics. A classical example is the use of topology to prove the existence of Nash equilibria [5]. More recently, tools from nonlinear algebra and algebraic geometry have given rise to *algebraic game theory*. In this framework, Nash equilibria can be computed via systems of multilinear equations [1, 3, 11]. Algebraic game theory thus provides algebraic tools for the study of equilibrium sets with semialgebraic structure. This extended abstract, based on [2] (submitted), focuses on the algebro-geometric study of totally mixed conditional independence equilibria.

Dependency equilibria form another important equilibrium concept with semialgebraic structure. Unlike Nash equilibria, which model independent and non-communicating players, dependency equilibria allow for coordinated, collective behavior. Introduced by Spohn [10], their geometric study was initiated in [8] through the associated Spohn variety, with further developments in [4, 9]. From a game-theoretic perspective, Nash and dependency equilibria lie at opposite extremes of the spectrum of player dependencies. This naturally raises the

J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, V. Sotomayor (eds.): Proceedings of the XIX EACA, pp. 211-215 (2026).
ISBN: 978-84-09-87277-0

question of whether intermediate equilibrium notions exist, for instance when players are partitioned into independent groups.

Totally mixed conditional independence (CI) equilibria provide such an intermediate concept. The key idea is to model dependencies among players using a graphical model in which vertices represent players, and edges encode dependency relations. In this framework, Nash equilibria correspond to noedge graphs, while dependency equilibria are associated with complete graphs. The concept of CI equilibria of a game and a graph G was first introduced in [8, Section 6] as the intersection of the probability simplex with the so-called *Spohn CI variety* of the game. The Spohn CI variety is obtained by first intersecting the Spohn variety with the undirected graphical model of the graph G, and then removing some possible irreducible components lying in certain undesired hyperplanes. In order to comprehend the behavior of CI equilibria, one first has to understand the geometry of Spohn CI varieties. The algebro-geometric study of Spohn CI varieties was proposed in [8, Section 6] where [8, Conjecture 24] conjectured a formula for the dimension of Spohn CI varieties for generic binary games. In [6], this formula and other properties were proven for binary games and one edge graphs. Later, [8, Conjecture 24] was proven in [7] for binary games and all graphs.

In this extended abstract, we present results from [2], where the study of Spohn CI varieties and CI equilibria is extended to arbitrary game formats and graphs. Theorem 1 generalizes [8, Conjecture 24] to all game formats, while Theorem 2 analyzes the smoothness of the set of totally mixed CI equilibria. We also study cluster graphs, i.e., disjoint unions of complete graphs, for which the Spohn CI variety is called the *Nash CI variety*. This corresponds to partitioning players into independent groups that behave collectively within each component. In this setting, we show that generic Nash CI varieties are irreducible and compute their defining equations, Chow class, and degree [2, Proposition 4.3, Theorem 4.4, Theorem 4.6, Proposition 4.7]. Finally, we address a key difficulty in the nonbinary case: the Spohn CI variety may be empty for generic games. While this never occurs for binary games, it does for certain nonbinary formats as shown in [1, Theorem 2.7] for the totally mixed Nash equilibria (noedge graphs). We extend this classical emptiness results to cluster graphs and characterize when generic Nash CI varieties are empty in Theorem 3.

Algebraic game theory

We work in the setting of *normal form finite n–player game*. Such a game is specified as follows. First, we fix the number of players $n \in \mathbb{N}$. For $i \in [n]$, the i–th player can select among d_i strategies, which determines the format of the game as $d_1 \times \cdots \times d_n$. The game is specified by fixing for each player $i \in [n]$ a real tensor $X^{(i)} \in V := \mathbb{R}^{d_1 \cdots d_n}$ called the *payoff table* of player i. The entry $X^{(i)}_{j_1 \cdots j_n}$ represents the payoff or benefit that the i–th player receives when player 1 chooses strategy j_1, player 2 chooses strategy j_2, and so on. Players participate in the game by collectively choosing a joint probability $P \in V$. The entry $p_{j_1 \cdots j_n}$ for $j_1 \in [d_1], \ldots, j_n \in [d_n]$ is the probability that player 1 chooses strategy j_1, player 2 chooses strategy j_2, etc.

A central theme in game theory is the study of different equilibrium notions. An equilibrium is a probability tensor in the simplex Δ of V satisfying constraints imposed by the game-theoretic setting. For many equilibrium concepts, these constraints are polynomial, motivating the use of algebraic geometry. Due to space limitations, we adopt an algebraic perspective and refer to [8, 11] for the corresponding game-theoretic definitions.

To apply algebro-geometric tools, we work in the projective space $\mathbb{P}(V)$ with coordinates $p_{j_1\cdots j_n}$ for $j_1 \in [d_1], \ldots, j_n \in [d_n]$. The quotient map $V \to \mathbb{P}(V)$, when restricted to the probability simplex Δ, induces a diffeomorphism onto its image, which we also denote by Δ. For each player $i \in [n]$ we consider the $d_i \times 2$ matrix

$$M^{(i)} = \begin{pmatrix} \sum_{j_1\in[d_1]} \cdots \widehat{\sum_{j_i\in[d_i]}} \cdots \sum_{j_n\in[d_n]} p_{j_1\cdots 1\cdots j_n} & \sum_{j_1\in[d_1]} \cdots \widehat{\sum_{j_i\in[d_i]}} \cdots \sum_{j_n\in[d_n]} X^{(i)}_{j_1\cdots 1\cdots j_n} p_{j_1\cdots 1\cdots j_n} \\ \vdots & \vdots \\ \sum_{j_1\in[d_1]} \cdots \widehat{\sum_{j_i\in[d_i]}} \cdots \sum_{j_n\in[d_n]} p_{j_1\cdots d_i\cdots j_n} & \sum_{j_1\in[d_1]} \cdots \widehat{\sum_{j_i\in[d_i]}} \cdots \sum_{j_n\in[d_n]} X^{(i)}_{j_1\cdots d_i\cdots j_n} p_{j_1\cdots d_i\cdots j_n} \end{pmatrix}.$$

The *Spohn variety* $\mathcal{V}_X$ of a game X is the variety of $\mathbb{P}(V)$ defined by the 2×2 minors of the matrices $M^{(1)}, \ldots, M^{(n)}$. We say that a tensor $P \in \mathbb{P}(V)$ is a *totally mixed dependency equilibrium* if it lies in the intersection of $\mathcal{V}_X \cap \Delta^\circ$ where Δ° is the interior of the simplex $\Delta \subset \mathbb{P}(V)$. In [8, Theorem 6], the following alternative algebraic definition of totally mixed Nash equilibria is given. A tensor $P \in \mathbb{P}(V)$ is a *totally mixed Nash equilibrium* if it lies in the intersection $\mathbb{P}^{d_1-1} \times \cdots \times \mathbb{P}^{d_n-1} \cap \mathcal{V}_X \cap \Delta^\circ$. Here, $\mathbb{P}^{d_1-1} \times \cdots \times \mathbb{P}^{d_n-1}$ is contained in $\mathbb{P}(V)$ through the Segre embedding. These two notions of equilibria represent two opposite extremes of the spectrum of dependencies between the players. Nash equilibria model the independence behavior of the players, and the dependency equilibria correspond to the collective behavior. The dependency gap between these two notions of equilibria is filled by the concept of CI equilibria where the dependencies are modeled by a graph whose vertices represent the players and the edges the dependencies. This modeling is done through the undirected graphical model $\mathcal{M}_G$ associated to the graph. Since we are focused on totally mixed equilibria (non zero probabilities), there is no distinction between the undirected graphical model coming from distinct Markov properties of the graph. Thus, the undirected graphical model $\mathcal{M}_G$ is a toric variety whose monomial parametrization is described through the maximal cliques of the graph (see [12]). The *Spohn conditional independence (CI) variety* $\mathcal{V}_{X,G}$ of a graph G and a game X is defined as the variety obtained by removing from the intersection $\mathcal{M}_G \cap \mathcal{V}_X$ the irreducible components lying in the hyperplanes

$$\left\{ \sum_{j_1\in[d_1],\ldots,j_n\in[d_n]} p_{j_1\cdots j_n} = 0 \right\} \quad \text{and} \quad \{p_{j_1\cdots j_n} = 0\} \ \text{ for every } j_1 \in [d_1], \ldots, j_n \in [d_n]. \tag{1}$$

For most graphs, the intersection $\mathcal{M}_G \cap \mathcal{V}_X$ is not irreducible and it has irreducible components lying in the hyperplanes (1) that complicates the geometry of the desired variety. The exclusion of these components from the Spohn CI variety arises from game-theoretic considerations. We say that a tensor $P \in \mathbb{P}(V)$ is a *totally mixed conditional independence (CI) equilibrium* if it lies in the intersection $\mathcal{V}_{X,G} \cap \Delta^\circ$. Understanding the set of totally mixed CI equilibria starts with the study of Spohn CI varieties. As mentioned in the introduction, this study was proposed in [8, Section 6] and for binary games it was done in [6, 7]. In this

extended abstract, based on the preprint [2], we extend the study of Spohn CI varieties to nonbinary games and all graphs. At this point, we note that to understand the above varieties defined over $\mathbb{R}$, we first consider them over $\mathbb{C}$ and study their properties over this field. We then derive information about their real points from the complex setting.

Main results

We summarize the main results of [2], which describe the generic behavior of the Spohn CI variety, i.e., for payoff tables in a dense Zariski open subset of V. The first result determines the dimension of Spohn CI varieties for generic nonbinary games, extending [8, Conjecture 24] (proved in [7, Theorem 9] for binary games) to arbitrary game formats.

Theorem 1. ([2, Theorem 3.6]) *Let G be a graph with n vertices. Then, either $\mathcal{V}_{X,G}$ is empty for a generic game X, or* $\operatorname{codim}_{\mathcal{M}_G} \mathcal{V}_{X,G} = d_1 + \cdots + d_n - n$ *for a generic game X.*

The strategy is to use the monomial parametrization of $\mathcal{M}_G$ to pull back the Spohn CI variety to a torus and compute its dimension there using noncomplete linear systems and Bertini's Theorem. From the study of these linear systems yields the following result.

Theorem 2. ([2, Theorem 3.7]) *Let G be a graph with n vertices. Then, for generic games the Spohn CI variety $\mathcal{V}_{X,G}$ is smooth away from the hyperplanes* (1)*. In particular, for generic games, the set of totally mixed CI equilibria is either empty or a smooth manifold of codimension $d_1 + \cdots + d_n - n$ in $\mathcal{M}_G$.*

At the level of ideals, the definition of the Spohn CI variety requires a saturation process that becomes computationally challenging when the format of the game increases. In [2, Section 3.3], we give a new set of hyperplanes for this saturation that improves the speed of the computation. Another issue arising from this saturation is the lack of equations for the Spohn CI variety, which complicates the study of these varieties. In [2, Proposition 4.3], we provide these equations for generic games and *cluster graphs*. For these graphs, $\mathcal{M}_G$ is a Segre variety and the Spohn CI variety is called the *Nash CI variety*. Using [2, Proposition 4.3] we show that Nash CI varieties are irreducible for generic games ([2, Theorem 4.4]), and we compute their Chow class and degree (see [2, Theorem 4.6, Proposition 4.7]). Using the Chow class, we extend the classical characterization [1, Theorem 2.7] of the emptyness of totally mixed Nash equilibria (no edge graphs) to all cluster graphs.

Theorem 3. ([2, Theorem 5.4]) *Let G be a cluster graph G whose connected components are $G_1, \ldots, G_k$. Then, the Nash CI variety is nonempty for generic games if and only if for every isolated vertex i*

$$d_i \leq 1 + \frac{1}{2}\sum_{l=1}^{k}(D_l - 1), \text{ where } D_l = \prod_{j \in G_l} d_j.$$

For example, consider a 3 players game with strategies d_1, d_2 and d_3. For the noedge graph (totally mixed Nash equilibria), the Nash CI variety is nonempty if and only if $d_1 \leq d_2 + d_3 - 1$, $d_2 \leq d_1 + d_3 - 1$ and $d_3 \leq d_1 + d_2 - 1$, whereas for the graph with one edge between players 2 and 3, the Nash CI variety is nonempty for generic games if and only if

$d_1 \leq d_2 d_3$. For instance, for $d_1 = 4$ and $d_2 = d_3 = 2$, the Nash CI variety of the noedge graph is empty, but for one-edge graph is a curve for generic games.

References

[1] H. Abo, I. Portakal, L. Sodomaco: A vector bundle approach to nash equilibria. *Adv. Appl. Math.* **175**, 103028 (2026).

[2] M. Bouyer, I. Portakal, J. Sendra-Arranz: Totally mixed conditional independence equilibria of generic games. *ArXiv:2511.11467* (2025).

[3] R.S. Datta: Universality of nash equilibria. *Math. Oper. Res.* **28**(3), 424–432 (2003).

[4] A. Kidambi, E. Neuhaus, I. Portakal: Elliptic curves in game theory. *ArXiv:2501.14612* (2025).

[5] J.F. Nash Jr.: Equilibrium points in n-person games. *Proc. Natl. Acad. Sci. USA* **36**(1), 48–49 (1950).

[6] I. Portakal, J. Sendra-Arranz: Nash conditional independence curve. *J. Symbolic Comput.* **122**, 102255 (2024).

[7] I. Portakal, J. Sendra-Arranz: Game theory of undirected graphical models. *J. Algebra* **666** (2025).

[8] I. Portakal, B. Sturmfels: Geometry of dependency equilibria. *Rend. Ist. Mat. Univ. Trieste* **54**(5), 26 pp. (2022).

[9] I. Portakal, D. Windisch: Dependency equilibria: Boundary cases and their real algebraic geometry. *Adv. Appl. Math.* **168**, 102890 (2025).

[10] W. Spohn: Dependency equilibria and the causal structure of decision and game situations. *Homo Oeconomicus* **20**, 195–255 (2003).

[11] B. Sturmfels: *Solving Systems of Polynomial Equations*. Conference Board of the Mathematical Sciences, Regional Conference Series in Mathematics **97**, Amer. Math. Soc. (2002).

[12] S. Sullivant: *Algebraic statistics*. Conference Board of the Mathematical Sciences, Regional Conference Series in Mathematics **194**, Amer. Math. Soc. (2023).

Posters

Quantum cryptographic protocols

B.H. Cáceres Barrera*†, P. Caballero-Gil*, D. Escanez-Exposito*, H.J. Reboso Morales*†, C. Caballero-Gil*

* *University of La Laguna*

† *Atlantis Tecnología y Sistemas, S.L.U.*

alu0101339368@ull.edu.es, pcaballe@ull.edu.es, jescanez@ull.edu.es, hreboso@atlantistecnologia.com, ccabgil@ull.edu.es

Cryptographic systems play a crucial role in information and communication security, as they ensure the confidentiality, integrity, and authenticity of transmitted data. The most basic cryptographic protocols, known as cryptographic primitives, are fundamental for constructing more complex and robust protocols. In this context, quantum computation has emerged as a powerful tool for implementing these protocols in a probabilistically secure manner. In this work, we introduce and analyze some of the most basic quantum cryptographic protocols found in the literature, exploring potential weaknesses and practical alternatives with more realistic assumptions under present-day technological constraints.

After an introductory exploration of some preliminaries of two-party cryptoprotocols and quantum computing, we have established that primitives such as oblivious transfer, bit commitment, and coin flipping cannot be implemented with strict security guarantees according to their theoretical definitions, both in classical and quantum settings [1]. Specifically, in the quantum realm, we examined early protocols based on the BB84 scheme [2]. As expected, these protocols exhibited significant security flaws, leading to discussions on the impracticality of achieving strict security in these quantum primitives. Nevertheless, we identified highly promising quantum alternatives where relaxing security conditions or limiting quantum memory storage could lead to significantly more secure protocols.

In particular, we investigated concepts such as quantum oblivious transfer with limited quantum memory [3], quantum coin flipping with bias [4], and weak quantum bit commitment [5]. Furthermore, we presented some simple protocols from the literature for each scenario to evaluate their security and provide concrete examples of potential attacks by dishonest Alice and Bob, thereby enhancing the understanding of each protocol's operation. This practical approach has enabled us to develop a thorough and detailed understanding of each proposed protocol, an aspect often not found in the papers due to their predominantly theoretical focus and the frequent absence of specific examples and attack analyses.

References

[1] B.H. Cáceres: *Quantum Cryptographic Protocols*. Master's thesis, University of La Laguna (2024).

J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, V. Sotomayor (eds.): Proceedings of the XIX EACA, pp. 217-218 (2026).
ISBN: 978-84-09-87277-0

[2] C.H. Bennett, G. Brassard: *Quantum cryptography: public key distribution and coin tossing*. International Conference on Computers, Systems and Signal Processing, 175–179 (1984).

[3] I.B. Damgård, S. Fehr, L. Salvail, C. Schaffner: Cryptography in the bounded-quantum-storage model. *SIAM J. Comput.* **37**(6), 1865–1890 (2008).

[4] A. Ambainis: *A new protocol and lower bounds for quantum coin flipping*. Proceedings of the thirty-third annual ACM symposium on theory of computing, 134–142 (2001).

[5] D. Aharonov, A. Ta-Shma, U.V. Vazirani, A.C. Yao: *Quantum bit escrow*. Proceedings of the thirty-second annual ACM symposium on theory of computing, 705–714 (2000).

Persistent homology applied to genetic study of populations

B.H. Cáceres Barrera*, C. González Alcón†, J. Remedios Gómez†
* *University of La Laguna, and Atlantis Tecnología y Sistemas S.L.U.*
† *Department of Mathematics, Statistics and Operations Research, University of La Laguna*
alu0101339368@ull.edu.es, jremed@ull.edu.es, galcon@ull.edu.es

Abstract. Topological Data Analysis is a discipline that combines concepts and techniques from topology with data analysis to study and understand the underlying structure in complex data sets. Its objective is to reveal important patterns and features that may be hidden in the data and are not easily detectable using traditional analysis methods. One of its most widely used tools is persistent homology, which detects relevant topological features through a filtration of simplicial complexes that can be generated from a point cloud. This technique of topological analysis has gained significant relevance in recent years and it is applied across a wide variety of scientific disciplines. In this work, we use the tools provided by persistent homology in the context of genetics to conduct a study among populations of *Coscinasterias tenuispina*, a species of starfish distributed iacross various regions of the Atlantic Ocean and the Mediterranean Sea.

Introduction

Topological Data Analysis (TDA) has emerged as a novel technique for studying and analyzing complex datasets in response to the growing need to develop innovative and efficient methods for processing massive amounts of data. In this context, persistent homology stands out as one of the fundamental tools of TDA, providing a unique perspective that allows us to explore the inherent structure of data and reveal complex patterns and hidden characteristics. This technique has found widespread application across various scientific fields. In particular, in the field of genetics, persistent homology offers a wealth of possibilities, such as the identification of groups of individuals with similar genetic profiles or the detection of subpopulations.

Thus, the main objective of this work [1] has been to use the theoretical principles of persistent homology in a computational context and to evaluate the added value that this technique can bring to the field of genetics.

Metodology and results

Below we present a brief summary of the methodology used, including both the basic concepts of persistent homology (for a more in-depth theoretical basis, see [2], [3], and [4])

J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, V. Sotomayor (eds.): Proceedings of the XIX EACA, pp. 219-223 (2026).
ISBN: 978-84-09-87277-0

and the computational tools used, as well as a brief presentation of the results achieved. To obtain a topological representation of our data, we used what are known as simplicial complexes. In this study, we can consider them as constructions based on a *point cloud* (understood as a finite subset of $\mathbb{R}^N$, which represents our data set) that will allow us to model the geometric structure of the data to obtain a representation of its spatial distribution.

In this work, we focus on the Vietoris-Rips complex, widely used in TDA given its computational efficiency. Specifically, the **Vietoris-Rips** complex associated with $S \subset \mathbb{R}^N$ and $r > 0$ is defined as

$$\mathrm{VR}(r) := \{\sigma \subseteq S / \mathrm{diam}(\sigma) \leq r\}$$

where $\mathrm{diam}(\sigma) = \max\{\mathrm{dist}(x, y)/x, y \in \sigma\}$ where dist is any distance function in $\mathbb{R}^N$.

By assigning different values to the free parameter $r > 0$, we obtain a family of nested simplicial complexes forming a filtration of simplicial complexes ($\mathrm{VR}(0) = \emptyset$).

$$\mathcal{VR}(S) = \{\mathrm{VR}(r)\}_{r \geq 0}$$

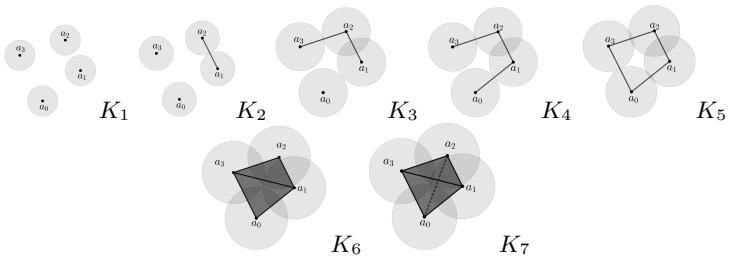


Figure 1. Example of Vietoris-Rips filtration.

The study of the persistence of topological characteristics such as connected components, holes, and voids (homology) throughout a filtration provides us with an idea of the structure of our data, and persistent homology is responsible for performing this analysis. Graphically, we can obtain the so-called persistence diagrams or associated barcodes (Figure 2) showing the persistence of these topological characteristics. They represent the birth and death of the topological characteristics mentioned above throughout a filtration of simplicial complexes.

From a computational point of view, there is a wide range of algorithm implementations and packages designed for persistent homology computation [5], available in different programming languages. In our particular case, we have chosen the TDA package (Statistical Tools for Topological Analysis) [6], which provides us with a series of R functions that allow us to apply efficient algorithms focused on the calculation of persistent homology.

Finally, we used persistent homology to study the genetic data of a species of starfish called *Coscinasterias tenuispina*. These starfish have a great capacity for dispersal and colonization through the combination of sexual and asexual cycles in their reproductive systems,

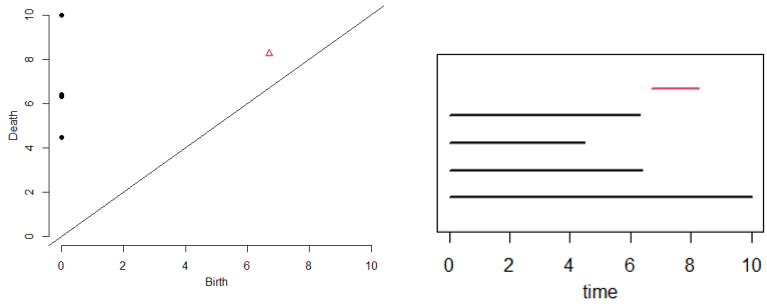


Figure 2. Persistence diagram (left) and barcode (right) associated with the filtration in Figure 1. The black colour represents the persistence of connected components and red represents the persistence of one-dimensional holes.

which has motivated the study of their population genetic structure. We studied the genetic relationships between 16 different populations in the Atlantic and Mediterranean, with a total of 405 individuals, based on the genetic data used in [7]. The samples were taken between 2010 and 2014.

To analyze possible genetic relationships between different populations using persistent homology tools, we use the R package `hierftstat` [8], which provides us, among other things, with the `genet.dist` function, which allows us to calculate the genetic distance between populations using the coefficient F_{ST} [9]. We set the different populations as vertices of the Vietoris-Rips filtration, so that each population is connected to the others in one order or another depending on the genetic distance between them, until finally forming a single connected component. Furthermore, in this case, the persistence index tells us how similar these populations will be. The higher the persistence index, the less related the populations that are joining (since they have been connected later).

Genetic information between the different populations that we have obtained is summarized in the following Figure 3.

Thus, it appears that the ALI (Alicante, Murcia), NAP (Naples, Campania), and LLA (Llançà, Girona) populations are genetically very close. The discussion section of [7] confirms the existence of a *superclone* (a dominant clonal lineage) that is widely distributed along the western Mediterranean coast of most of the populations studied in the area, from Alicante to Naples. Our results seem to confirm this fact.

On the other hand, it could be expected that the populations corresponding to the Canary Islands would be more genetically similar to each other than to the Mediterranean populations. However, we find that SIC (Taormina, Sicily) and LAN (Playa Blanca, Lanzarote) have less genetic differentiation than TAZ (Tazacorte, La Palma) and ABA (Abades, Tenerife), which could indicate a certain dispersion of larvae between Lanzarote and populations geograph-

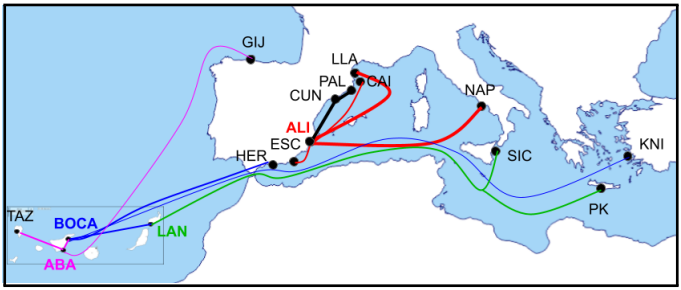


Figure 3. Related components obtained from populations of C. tenuispina (in cases where we had two samples from the same population, the most recent sample is shown in this figure). The thicker the line, the greater the genetic relationship (and therefore the lower the filtration value). The color of each line indicates the destination population in each connection (except for the black lines, which indicate clonal populations). For example, the line that starts at GIJ joins ABA (pink) and corresponds to the GIJ-ABA connection obtained in the filtering with a value of 0.3829.

ically far removed from the Mediterranean. This fact confirms the great dispersal capacity that larvae can have through ocean currents, as discussed in [7]. Furthermore, geographical proximity does not necessarily imply genetic proximity, since, as we have seen, this species has a great dispersal capacity and it could be that the larvae end up in places that are geographically very distant from the population of origin.

Acknowledgements. The first author has been partially supported by a research collaboration grant.

References

[1] B.H. Cáceres: *Persistent homology applied to genetic study of populations.* Bachelor's thesis, University of La Laguna (2023).

[2] H. Edelsbrunner, J.L. Harer: *Computational topology: an introduction.* American Mathematical Society (2010).

[3] J.R. Munkres: *Elements of algebraic topology.* CRC Press (2018).

[4] A. Zomorodian, G. Carlsson: Computing persistent homology. *Discrete Comput. Geom.* **33**(2), 249–274 (2005).

[5] N. Otter, M.A. Porter, U. Tillmann, P. Grindrod, H.A. Harrington: A roadmap for the computation of persistent homology. *EPJ Data Sci.* **6**, 1–38 (2017).

[6] B.T. Fasy, J. Kim, F. Lecci, C. Maria, D.L. Millman, V. Rouvreau, M.J. Kim: *TDA: Statistical Tools for Topological Data Analysis.* R package version 1.9. `https://CRAN.R-project.org/package=TDA` (2023).

[7] R. Pérez-Portela, A. García-Cisneros, M. Campos-Cañet, C. Palacín: Genetic homogeneity, lack of larvae recruitment, and clonality in absence of females across western Mediterranean populations of the starfish *Coscinasterias tenuispina*. *Sci. Rep.* **11**, 16819 (2021).

[8] J. Goudet, T. Jombart, M.J. Goudet: *hierfstat: Estimation and Tests of Hierarchical F-Statistics*. R package version 0.5-11. `https://CRAN.R-project.org/package=hierfstat` (2022).

[9] N. Takezaki, M. Nei: Genetic distances and reconstruction of phylogenetic trees from microsatellite DNA. *Genetics* **144**(1), 389–399 (1996).

Estudio de singularidades de curvas planas vía el loto asociado

I. González Rodríguez
Universidad de La Laguna
alu0101474212@ull.edu.es

El estudio de las singularidades de curvas planas ha evolucionado significativamente desde las primeras clasificaciones de Newton en el siglo XVII sobre nodos y cúspides. Tras la formalización de la resolución de singularidades por Heisuke Hironaka en el siglo XX, han surgido herramientas combinatorias modernas para describir este proceso. En el siglo XXI, Evelia R. García Barroso, Pedro D. González Pérez, Patrick Popescu-Pampu crean el loto, un objeto geométrico que codifica este proceso. El objetivo de este trabajo consiste en presentar el computo del loto y analizar su relación con la resolución de singularidades de curvas planas.

J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, V. Sotomayor (eds.): Proceedings of the XIX EACA, pp. 224-224 (2026).
ISBN: 978-84-09-87277-0

The v-number of ideals associated to graphs

D. Jaen Guedes, M.S. García Román, D. Jaramillo-Velez
Universidad de La Laguna y Atlantis Tecnología y Sistemas S.L.U.
alu0101360676@ull.edu.es, mgarciro@ull.edu.es, djaramil@ull.edu.es

A graph is characterized not only by its edges, but also by its invariants, such as the independence number, domination number, cover number, and others. In most cases, computing these invariants is an NP-hard problem. For this reason, seeking new interpretations of these concepts is a relevant and worthwhile endeavor. In particular, algebraic interpretations are especially valuable, as they may lead to algorithmic approaches for computing these invariants [2].

Concrete examples of this interplay arise in the study of the v-number and edge ideals. It is known that the independence number of a graph coincides with the v-number of its edge ideal, while the connected domination number coincides with the v-number of the binomial edge ideal [2, 3].

Algorithms for estimating the v-number have been implemented in computer algebra systems such as Macaulay2, providing practical tools to experiment with and compute graph invariants through algebraic methods [1, 4].

In this poster, we present a brief introduction to the concept of the v-number, including its connections to coding theory and recent results on its combinatorial interpretations.

We analyze the relationship between the v-number of edge ideals and the v-number of binomial edge ideals, highlighting the corresponding relationship between the independence number and the connected domination number. Finally, we present computations and insights concerning the v-number of other graph-associated ideals, such as neighborhood ideals and weighted edge ideals. Our hypotheses are supported by computational results obtained using the v-number function from the Coding Theory package in Macaulay2.

References

[1] T. Ball, et al.: *Coding theory package for Macaulay2*. J. Softw. Algebra Geom. **11**(1), 113–122 (2022).

[2] D. Jaramillo, R.H. Villarreal: The v-number of edge ideals. *J. Combin. Theory Ser. A* **177**, 105310 (2021).

[3] D. Jaramillo-Velez, L. Seccia: Connected domination in graphs and v-numbers of binomial edge ideals. *Collect. Math.* **75**(3), 771–793 (2024).

[4] S.M. Cooper, et al.: Generalized minimum distance functions and algebraic invariants of Geramita ideals. *Adv. Appl. Math.* **112**, 101940 (2020).

J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, V. Sotomayor (eds.): Proceedings of the XIX EACA, pp. 225-225 (2026).
ISBN: 978-84-09-87277-0

Some families of optimal pure quantum (r, δ)-LRCS

H. Martín-Cruz
Universidad de Jaén
hmartin@ujaen.es

Classical (r, δ)-locally recoverable codes are designed for avoiding loss of information in large scale distributed and cloud storage systems. We introduce the quantum counterpart of those codes by defining quantum (r, δ)-locally recoverable codes which are quantum error-correcting codes capable of correcting $\delta - 1$ qudit erasures from sets of at most $r + \delta - 1$ qudits.

We give a necessary and sufficient condition for a quantum stabilizer code $Q(C)$ to be (r, δ)-locally recoverable. Our condition depends only on the puncturing and shortening at suitable sets of both the symplectic self-orthogonal code C used for constructing $Q(C)$ and its symplectic dual $C^{\perp_s}$. When $Q(C)$ comes from a Hermitian or Euclidean dual-containing code, and under an extra condition, we show that there is an equivalence between the classical and quantum concepts of (r, δ)-local recoverability. A Singleton-like bound is stated in this case. It shows that it suffices to provide an optimal Euclidean (or Hermitian) dual-containing (r, δ)-LRC giving rise to a pure quantum stabilizer code, for having an optimal (pure) quantum (r, δ)-LRC.

In this poster we focus on the Euclidean construction using $\emptyset$-affine variety codes which are optimal (r, δ)-LRCs [1]. Therefore they give rise to optimal pure quantum (r, δ)-LRCs. This is a joint work with C. Galindo, F. Hernando and R. Matsumoto [2].

References

[1] C. Galindo, F. Hernando, H. Martín-Cruz: Optimal (r, δ)-LRCs from monomial Cartesian codes and their subfield-subcodes. *Des. Codes Cryptogr.* **92**, 2549–2586 (2024).

[2] C. Galindo, F. Hernando, H. Martín-Cruz, R. Matsumoto: Quantum (r, δ)-locally recoverable codes. *Finite Fields Appl.* **111**, 102785 (2026).

J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, V. Sotomayor (eds.): Proceedings of the XIX EACA, pp. 226-226 (2026).
ISBN: 978-84-09-87277-0

Nilpotency and topological complexity

J.F. Pineda Ramos
University of La Laguna
jpinedar@ull.edu.es

Farber's topological complexity $\mathrm{TC}(X)$ is a homotopy invariant defined in terms of the existence of local sections of the path fibration over $X \times X$. While upper bounds for $\mathrm{TC}(X)$ can often be obtained constructively by exhibiting suitable open covers of $X \times X$, lower bounds are more subtle: failing to produce a small cover does not prove that such a cover does not exist.

In this poster we highlight an algebraic approach to lower bounds based on the graded–commutative cohomology algebra $A = H^*(X; R)$. Considering the multiplication map

$$\mu : A \otimes_R A \longrightarrow A,$$

the kernel $Z = \ker(\mu)$ forms the ideal of zero divisors in $A \otimes_R A$. The nilpotency index of this ideal provides an effective lower bound for $\mathrm{TC}(X)$, turning a topological non-existence problem into a computable invariant of a graded algebra.

We present this construction from an algebraic perspective and illustrate how ring-theoretic properties of $H^*(X; R)$ influence $\mathrm{TC}(X)$. Several classical families of spaces are discussed, including spheres, projective spaces, surfaces, graphs, and configuration spaces, where the nilpotency bound yields sharp or near-sharp estimates.

J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, V. Sotomayor (eds.): Proceedings of the XIX EACA, pp. 227-227 (2026).
ISBN: 978-84-09-87277-0

Quantum synchronizable codes from polycyclic codes

M. de los Ríos, E. Martínez
Universidad de Valladolid
miguel.rios@estudiantes.uva.es, miguel.rios@estudiantes.uva.es

Quantum Synchronizable Codes (QSCs) are a specialized class of quantum codes designed to correct both Pauli errors and block misalignments. In[2], a framework for QSCs was established based on the CSS construction using dual-containing cyclic codes. Since cyclic codes can be viewed as ideals in the ring $\mathbb{F}_q[x]/\langle x^n - 1\rangle$, their algebraic structure provides a powerful tool for determining the correction capabilities.

In this work, we generalize this construction by considering more general algebraic structures. Specifically, we extend the QSC framework to polycyclic codes[1], which are ideals in rings of the form $\mathbb{F}_q[x]/\langle f(x)\rangle$ for a non-zero polynomial $f(x)$. This family of codes offers broader flexibility in error correction, potentially at the cost of its synchronization capabilities. This tradeoff is analyzed through simulations across a variety of different channels.

References

[1] N. Aydin, P. Liu, B. Yoshino: Polycyclic codes associated with trinomials: good codes and open questions. *Des. Codes Cryptogr.* **90**, 1241–1269 (2022).

[2] Y. Fujiwara, V.D. Tonchev, T.W.H. Wong: Algebraic techniques in designing quantum synchronizable codes. *Phys. Rev. A* **88**, 012318 (2013).

J. Gómez-Torrecillas, F.J. Lobillo, G. Navarro, V. Sotomayor (eds.): Proceedings of the XIX EACA, pp. 228-228 (2026).
ISBN: 978-84-09-87277-0