



EACA2024 - Schedule

Monday, June 24

- 9:00-9:30 Registration/Opening
- 9:30 -10:30 Plenary - **Diane Maclagan**: *Computational algebra in tropical geometry*
- 10:30-11:00 Coffee
- 11:00-11:30 Room 1 - M. Bender, L. Buse, C. Checa, E. Tsigaridas: *Multigraded Castelnuovo-Mumford regularity and Gröbner bases*
Room 2 - D. Miguel, A. Guidolin and A. Romero: *Stable rank analysis applied to semi-supervised learning*
- 11:30-12:00 Room 1 - I. García-Marco, P. Gimenez, M. González-Sánchez: *Betti numbers of projective and affine monomial curves*
Room 2 - E. Álvarez-González: *Demostración de Fórmulas de Ajuste basadas en el Algoritmo Más Cercano*
- 12:00-12:30 Room 1 - C. D'Andrea, G. Jeronimo: *Sparse Nullstellensatz, resultants and determinants of complexes*
Room 2 - E. Camacho-Aguilar, F. Castro-Jiménez, F. García-Cortés: *Algebraic methods in cell differentiation*
- 12:30-13:00 Room 1 - H. Lombardi: *Some classical results in Algebra needing one or several constructive versions*
Room 2 - Y. Mukhina, G. Pogudin: *Support of the Minimal Polynomial in the Differential Dynamical System*
- 13:00-15:00 Lunch
- 15:00-16:00 Plenary - **Martin Avendaño**: *The DME cryptosystem*
- 16:00-17:00 Coffee & **Poster Session**
- C. Checa, L. Busé: *Toric Sylvester forms*
 - Luengo, M. Avendaño, P. Coscojuela: *DME⁽⁻⁾-sign: a new DME cryptosystem for signatures*

- J. Rodríguez: *Inflection points of algebraic surfaces, a modern approach to the work of George Salmon.*
- D. Rojas, L. Hernández: *Analysis of the crystals-kyber implementation*

- 17:00-17:30 Room 1 - S. Pérez-Díaz: *Generalized asymptotes of parametric curves*
Room 2 - A. Fidalgo-Díaz, U. Martínez-Peñas: *Distributed matrix multiplication over small fields with straggler tolerance*
- 17:30-18:00 Room 1 - L. Busé, P. González-Mazón: *Construction of birational trilinear volumes via tensor rank criteria*
Room 2 - U. Martínez-Peñas, R. Rodríguez-Ballesteros: *Hamming Weight Distributions of Codes that are Linear over a Subfield*
- 18:00-18:30 Room 1 - R. Iglesias, M. Orth, E. Sáenz-de-Cabezón: *Algorithms on Janet-like bases*
Room 2 - I. Blanco-Chacón, R. Durán-Díaz, R. M. Sánchez-Ledesma: *Overview and extension of root-based attacks against PLWE instances*
- 18:30-19:00 Room 1 - A. Fernandez-Boix, D. Gómez-Ramírez: *Frobenius algebras of rings of prime characteristic: a quick tour*
Room 2 - D. Ruano, R. San-José: *About the hulls of projective Reed-Muller codes*

Tuesday, June 25

- 9:00-10:00 Plenary - **Anton Leykin**: *Inexact methods in nonlinear algebra*
- 10:00-10:30 Room 1 - J. A. Delgado, A. Romero, J. Rubio, F. Sergeraert: *Upper bounds for the homology of $K(Z, n)$ and $K(Z/mZ, n)$*
Room 2 - T. Recio, M.P. Vélez: *A real mechanical geometer*
- 10:30-11:00 Coffee
- 11:00-11:30 Room 1 - D. Senovilla: *Bases de Saito para una curva con un par de Puiseux*
Room 2 - F. Botana, T. Recio, M. P. Vélez: *GeoGebra Discovery and ChatGPT*
- 11:30-12:00 Room 1 - E. Pérez Callejo: *Exploring the dicritical configurations of extended planar foliations*
Room 2 - T. del Río: *Using Explainable AI to Extract Insights on Algebraic Procedures: a case study on variable ordering for CAD*
- 12:00-12:30 Room 1 - M. González-Regadera, M. D. Frau, R. Falcón: *Hadamard quasigroup products preserving the Latin square condition*

- Room 2 - V. Alvarez-Aparicio, M. T. Rivas-Rodríguez, L. J. Hernández-Paricio: *Algorithms and groupoids for the combinatorial classification of complex polynomials*
- 12:30-13:00 Room 1 - F. Mohammadi, O. Clarke, G. Masiero: *Defining Equations of Point Configurations*
- Room 2 - A. Pereira-Albert, T. Recio, M.P. Vélez: *Dealing with non-principal locus in automated reasoning in geometry*
- 13:00-15:00 Lunch
- 15:00-16:00 Plenary - **Lalo González-Vega**: *Closed-Form Formulae for the Conics/Quadrics Interference Problem through Quantifier Elimination*
- 16:00-16:30 Coffee
- 17:00- 20:00 Social program - Visit to the [Royal Site of San Lorenzo de El Escorial](#): Historical Royal Library and other areas
- 21:00-.. Social dinner - [Restaurante La Rueda](#)

Wednesday, June 26

- 9:30 -10:30 Plenary - **Alessandra Bernardi**: *An Algorithmic Approach to Cactus Rank and Its Implications for Complexity Theory*
- 10:30-11:00 Coffee
- 11:00-11:30 Room 1 - J. I. García, A. Vigneron, R. Tapia: *Over the quotient of C-semigroups*
- Room 2 - R. E. Mira-García, A. Díaz-Cano: *A new criterion for the positivity of symmetric polynomials of degree 6*
- 11:30-12:00 Room 1 - F. Mohammadi, E. Liwski: *Paving Matroids: Defining Equations and a Decomposition of Associated Matroid and Circuit Varieties*
- Room 2 - I. García-Marco, I. Márquez-Corbella, D. Seco: *On the number of Toeplitz factors of a matrix*
- 12:00-12:30 Room 1 - B. Guerville-Ballé, J. Viu-Sos: *A combinatorial approach to moduli spaces of line arrangements*
- Room 2 - S. Asensio, I. García-Marco, K. Knauer: *On the sensitivity of trilean functions*
- 12:30-13:00 Room 1 - F. Oviaño-García, R. Campoamor-Stursberg: *Enfoque computacional en el estudio de la rigidez de álgebras de Lie reales resolubles de rango uno*
- Room 2 - E. Briand, M. Rosas, L. Esquivias, A. Gutiérrez, A. Lillo: *Determinant of the distance matrix of a tree*
- 13:00-13:15 Closing

CONTENTS

Schedule	i
Contents	iv
Plenary Conferences	
Martín Avendaño	
<i>The DME cryptosystem</i>	vii
Alessandra Bernardi	
<i>An Algorithmic Approach to Cactus Rank and Its Implications for Complexity Theory</i>	viii
Anton Leykin	
<i>Inexact methods in nonlinear algebra</i>	ix
Lalo González Vega	
<i>Closed-Form Formulae for the Conics/Quadrics Interference Problem through Quantifier Elimination</i>	x
xiDiane MacLagan	
<i>Computational algebra in tropical geometry</i>	xi
Extended Abstracts	
Víctor Álvarez-Aparicio, María Teresa Rivas-Rodríguez and Luis Javier Hernández-Paricio	
<i>Algorithms and groupoids for the combinatorial classification of complex polynomials</i>	1
Ernesto Álvarez González	
<i>Proofs of approximation formulas based on the closest tree algorithm</i>	5
Sara Asensio, Ignacio García-Marco and Kolja Knauer	
<i>On the sensitivity of trilean functions</i>	9
Matías Bender, Laurent Buse, Carles Checa and Elias Tsigaridas	
<i>Multigraded Castelnuovo-Mumford regularity and Gröbner bases</i>	13
Iván Blanco Chacón, Raúl Durán Díaz and Rodrigo Martín Sánchez Ledesma	
<i>Overview and extension of root-based attacks against PLWE instances</i>	17
Francisco Botana, Tomas Recio and M. Pilar Velez	
<i>Geogebra discovery and CHATGPT</i>	22
Emmanuel Briand, Mercedes Rosas, Luis Esquivias, Alvaro Gutiérrez and Adrián Lillo	
<i>Determinant of the distance matrix of a tree</i>	26
Laurent Busé, Pablo González-Mazón	
<i>Construction of birational trilinear volumes via tensor rank criteria</i>	30
Elena Camacho-Aguilar, Francisco Castro-Jiménez and Francisco García-Cortés	
<i>Algebraic methods in cell differentiation</i>	34
Carlos D'Andrea and Gabriela Jeronimo	
<i>Sparse Nullstellensatz, resultants and determinants of complexes</i>	38
Juan Antonio Delgado, Ana Romero, Julio Rubio and Francis Sergeraert	
<i>Upper bounds for the homology of $K(Z, n)$ and $K(Z/mZ, n)$</i>	42
Alberto Fernandez Boix and Danny Gómez Ramírez	
<i>Frobenius algebras of rings of prime characteristic: a quick tour</i>	46
Adrián Fidalgo-Díaz and Umberto Martínez-Peñas	
<i>Distributed matrix multiplication over small fields with straggler tolerance</i>	50
Juan Ignacio García García, Alberto Vigneron Tenorio and Raquel Tapia Ramos	
<i>Over the quotient of C-semigroups</i>	54
Ignacio García-Marco, Philippe Gimenez and Mario González-Sánchez	
<i>Betti numbers of projective and affine monomial curves</i>	58
Ignacio García Marco, Irene Márquez Corbella and Daniel Seco	
<i>On the number of Toeplitz factors of a matrix</i>	62
Manuel González-Regadera, María Dolores Frau and Raúl Falcón	
<i>Hadamard quasigroup products preserving the Latin square condition</i>	66

Benoit Guerville-Ballé and Juan Viu-Sos	
<i>A combinatorial approach to moduli spaces of line arrangements</i>	70
Rodrigo Iglesias, Matthias Orth and Eduardo Sáenz-de-Cabezón	
<i>Algorithms on Janet-like bases</i>	74
Henri Lombardi	
<i>Some classical results in Algebra needing one or several constructive versions</i>	78
Umberto Martínez-Peñas and Rubén Rodríguez-Ballesteros	
<i>Hamming Weight Distributions of Codes that are Linear over a Subfield</i>	83
Daniel Miguel, Andrea Guidolin and Ana Romero	
<i>Stable rank analysis applied to semi-supervised learning</i>	87
Romualdo E. Mira García and Antonio Díaz-Cano Ocaña	
<i>A new criterion for the positivity of symmetric polynomials of degree 6</i>	91
Fatemeh Mohammadi, Oliver Clarke and Giacomo Masiero	
<i>Defining Equations of Point Configurations</i>	95
Emiliano Liwski and Fatemeh Mohammadi	
<i>Paving Matroids: Defining Equations and a Decomposition of Associated Matroid and Circuit Varieties</i>	99
Yulia Mukhina and Gleb Pogudin	
<i>Support of the Minimal Polynomial in the Differential Dynamical System</i>	103
Francisco Oviaño García and Rutwig Campoamor-Stursberg	
<i>Enfoque computacional en el estudio de la rigidez de álgebras de Lie reales resolubles de rango uno.</i>	107
Álvaro Pereira-Albert, Tomás Recio and M. Pilar Vélez	
<i>Dealing with non-principal locus in automated reasoning in geometry</i>	111
Elvira Pérez Callejo	
<i>Exploring the dicritical configurations of extended planar foliations</i>	115
Sonia Pérez-Díaz	
<i>Generalized asymptotes of parametric curves</i>	119
Tomas Recio and M. Pilar Velez	
<i>A real mechanical geometer</i>	123
Tereso del Río	
<i>Using Explainable AI to Extract Insights on Algebraic Procedures</i>	127
Diego Ruano and Rodrigo San-José	
<i>About the hulls of projective Reed-Muller codes</i>	131
David Senovilla	
<i>Bases de Saito para una curva con un par de Puiseux</i>	135

Posters

Carles Checa	
<i>Toric Sylvester forms</i>	140
Pilar Coscojuela Escanilla	
<i>DME(-)-sign: a new DME cryptosystem for signatures</i>	141
Diego Rojas Rodríguez	
<i>Analysis of the crystals-kyber implementation</i>	142
Jorge Rodríguez Pérez	
<i>Inflection points of algebraic surfaces, a modern approach to the work of George Salmon</i>	146

Plenary Conferences

THE DME CRYPTOSYSTEM

MARTÍN AVENDAÑO

ABSTRACT. The current and accelerated progress in quantum computing suggests that a real implementation of Shor's algorithm is very close to being achieved. This algorithm is capable of breaking the standard public-key cryptosystems based on factorization of integers and discrete logarithms. For this reason, a call for new quantum resistant public-key cryptosystems was launched by the American agency NIST. The goal of this talk is to present the DME cryptosystem, developed by Ignacio Luengo, that was submitted to the NIST competition. This cryptosystem can be used for encryption/decryption, signatures and KEM (key encapsulation). While standard public-key cryptography depends on the difficulty of factoring integers, the security of the DME cryptosystem is based on the difficulty of decomposing a composition of invertible polynomial maps over finite fields.

Universidad Complutense, Madrid, Spain
Email address: mavend01@ucm.es

AN ALGORITHMIC APPROACH TO CACTUS RANK AND ITS IMPLICATIONS FOR COMPLEXITY THEORY

ALESSANDRA BERNARDI

ABSTRACT. In this talk, I will present recent advancements in the computation of generalized additive decompositions of polynomials and their connection to cactus rank. I will highlight the significance of developing efficient algorithms for computing cactus rank, showing its relevance through connections to matrix multiplication in complexity theory.

University of Trento, Italy
Email address: `alessandra.bernardi@unitn.it`

INEXACT METHODS IN NONLINEAR ALGEBRA

ANTON LEYKIN

ABSTRACT. The classical framework of computational algebraic geometry is founded on Gröbner bases, resultants, and other symbolic constructions and algorithms which are typically executed in exact arithmetic. The output from an exact algebraic computation is generally assured to be correct.

Numerical algebraic geometry, in contrast, employs randomization and iterative methods of numerical analysis implemented in floating-point arithmetic. The correctness of the results obtained by such numerical algorithms can't be guaranteed automatically.

We will discuss several applications for which being correct every time is not an absolute necessity and, on the other hand, highlight several scenarios where formal verification of inexact results can be accomplished.

The work (joint with Christian, Duff, and Mancini) on initial orbit determination from line-of-sight measurements, a classical problem in astrodynamics, will serve as an illustration of a real-world application.

The second major illustration will come from the work (joint with Burr and Lee) on isolating clusters of zeros of analytic systems of equations using inflation, which develops a methodology to rigorously certify solutions to near-singular systems.

Georgia Institute of Technology, USA
Email address: leykin@math.gatech.edu

CLOSED-FORM FORMULAE FOR THE CONICS/QUADRICS INTERFERENCE PROBLEM THROUGH QUANTIFIER ELIMINATION

LAUREANO GONZÁLEZ VEGA

ABSTRACT. The problem of detecting when two moving conics/quadrics overlap is of interest to robotics, CAD/CAM, computational physics, computer animation, computer vision, ... where conics/quadrics are often used for modelling and/or enclosing the shape of the (more complex) objects under consideration. Since the sign of the real roots of the characteristic polynomial of the pencil defined by the two considered conics/quadrics determine when they overlap, are separate, or touch each other externally, searching closed-form formulae in the coefficients of the equations defining the considered conics/quadrics characterising when they do not share an interior common point, is a quantifier elimination problem over the reals. We will show how to solve symbolically this quantifier elimination problem (by using only subresultants and Descartes Rule of Signs), what is the current state of the art when looking for the best (those involving a smaller set of polynomials and/or less sign conditions) formulae dealing with this problem and how this solution can be used to solve the moving conics/quadrics problem before mentioned.

CUNEF, Madrid, Spain

Email address: laureano.gonzalez@cunef.edu

COMPUTATIONAL ALGEBRA IN TROPICAL GEOMETRY

DIANE MACLAGAN

ABSTRACT. Tropical geometry is a combinatorial shadow of algebraic geometry, in which varieties are replaced by their image under a valuation. In this talk I will give brief introductions to three different computational problems arising in tropical geometry. The first two involve computing tropical varieties: computing Groebner bases with valuations and the resulting polyhedral computations, while the third arises through the connection of matroids to tropical geometry.

Univ. Warwick, UK

Email address: `D.Maclagan@warwick.ac.uk`

Extended Abstracts

ALGORITHMS FOR THE COMBINATORIAL CLASSIFICATION OF COMPLEX POLYNOMIALS

V. ÁLVAREZ-APARICIO, L.J. HERNÁNDEZ-PARICIO, AND M.T. RIVAS-RODRÍGUEZ

ABSTRACT. The classification of different families of polynomials is already a classical problem that has been addressed in the literature by many different approaches. Many different combinatorial models and algebraic constructions have been considered for the sake of classification of polynomial maps. In this work, we will use the language of Category Theory and groupoids to give a combinatorial classification of complex polynomials with its critical values contained in a fixed finite set V .

In particular, we will say that two polynomials P and Q are equivalent if there is an affine transformation of the complex plane h such that $P = Qh$. The combinatorial classification will be achieved in terms of groupoid equivalence between the groupoid of complex polynomials of degree n with its critical values contained in V , and a certain finite groupoid of tuples of permutations of the symmetric group S_n satisfying some restrictions, called constellations. The fact that the latter is a finite groupoid allows us to design and implement algorithms of algebraic nature that can classify and compute different algebraic invariants associated with complex polynomials. In particular, some computations and a complete classification table will be presented for low-degree polynomials with at most 3 critical values, a classical example known in the literature as Shabat polynomials.

INTRODUCTION

Let $P: \hat{\mathbb{C}} \rightarrow \hat{\mathbb{C}}$, where $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ denotes the augmented complex plane, be the analytic map induced by a polynomial of $\deg(P) \geq 2$. Associated to P , one has the set of critical points of P , $C(P) = \{c \mid P'(c) = 0\} \cup \{\infty\}$, where P' denotes the derivative of P , and the set of critical values of P , $V(P) = \{P(c) \mid c \in C(P)\}$. It is well-known that the map $P|_{\hat{\mathbb{C}} \setminus P^{-1}(V(P))}: \hat{\mathbb{C}} \setminus P^{-1}(V(P)) \rightarrow \hat{\mathbb{C}} \setminus V(P)$ is a covering map with connected covering space. Moreover, the map $P: \hat{\mathbb{C}} \rightarrow \hat{\mathbb{C}}$ can be obtained either as the Freudenthal's compactification ([4]) or as the Fox's completion ([3]) of the map $P|_{\hat{\mathbb{C}} \setminus P^{-1}(V(P))}$.

Any non-critical value b_0 induces a canonical action (called monodromy action) over the permutation group of the fiber of b_0 , $\pi \rightarrow \text{Aut}(P^{-1}(b_0))$, where π denotes the fundamental group of $(\hat{\mathbb{C}} \setminus V(P), b_0)$. Considering a family of loops based on b_0 around each $q_i \in V(P)$, one can construct a canonical set of generators of the free group π and the action that each loop induces over $\text{Aut}(P^{-1}(b_0))$.

Given two non-constant complex polynomials $P(z), Q(z)$ we will say that P is equivalent to Q (or equivalent as branched coverings) if there are $a, b \in \mathbb{C}$ such that $a \neq 0$ and

The authors have been partially supported by the project PID2020-118753GB-I00 of the Spanish Ministerio de Ciencia e Innovación and the University of La Rioja REGI22/63.

The talk at the meeting EACA 2024 has been given by V. Álvarez-Aparicio.

$P(z) = Q(az+b)$; that is, if there exists an affine transformation h given by $h(z) = az+b$ such that $P = Qh$. Regarding this notion of equivalence, different terminologies as topological equivalence or Arnold equivalence can be found in the literature.

The classification of non-constant polynomials with critical values contained in a given finite set $V \subset \hat{\mathbb{C}}$ under different notions of equivalence has been widely studied by many researchers, for example, for the particular case with three critical values $V = \{q_1, q_2, \infty\}$, the so-called generalized Chebyshev polynomials, or Shabat polynomials, are obtained. For studies and classification of Shabat polynomials we refer the reader to [5], [6].

The aim of this work is to study this notion of monodromy in order to provide a combinatorial classification of non-constant polynomials, modulo equivalence, in terms of groupoids. Thereby, our main results are expressed with the terminology of groupoids and groupoid equivalences. In particular, we shall construct functors between certain groupoids of non-constant polynomials and some finite groupoids of combinatorial nature in order to prove the equivalence of their respective isomorphism classes (that is, in order to give a classification modulo equivalence). Moreover, these functors also provide an isomorphism between the automorphism group of a non-constant polynomial and the automorphism group of its associated combinatorial object in a finite groupoid. Benefitting from the finiteness of these combinatorial groupoids we are able to use the presented theory to explicit the considered classification for non-constant complex polynomials of low degree and to provide some examples.

1. CLASSIFICATION AND EQUIVALENCE OF GROUPOIDS

For each $n \in \mathbb{N}$, $n \geq 1$, we define the groupoid $\mathbf{BPol}_n$ that has as objects non-constant polynomial maps $P: \hat{\mathbb{C}} \rightarrow \hat{\mathbb{C}}$ of degree n . Given $P: \hat{\mathbb{C}} \rightarrow \hat{\mathbb{C}}$, $Q: \hat{\mathbb{C}} \rightarrow \hat{\mathbb{C}}$, a morphism in $\mathbf{BPol}_n$ is an affine map $u: \hat{\mathbb{C}} \rightarrow \hat{\mathbb{C}}$, $u(z) = az + b$, $a \neq 0$, such that the following diagram is commutative:

$$\begin{array}{ccc} \hat{\mathbb{C}} & \xrightarrow{u} & \hat{\mathbb{C}} \\ & \searrow P & \swarrow Q \\ & \hat{\mathbb{C}} & \end{array}$$

Fixing a finite set of points $V \subset \hat{\mathbb{C}}$ such that $\infty \in V$, we can consider the set of non-constant polynomials P of degree n such that $V(P) \subset V$, giving rise to the corresponding sub-groupoid of $\mathbf{BPol}_n$:

$$\mathbf{BPol}_n(\subset V).$$

Furthermore, if we consider the set of polynomials P of degree n such that $V(P) = V$, we have the following sub-groupoid:

$$\mathbf{BPol}_n(V).$$

From now on, we will denote by S_n the symmetric group of n elements; that is, the group of permutations of the canonical finite set $\{1, 2, \dots, n\}$. Also, we will write the product of permutations from left to right, and the image of a permutation $\sigma \in S_n$ in a point $j \in \{1, 2, \dots, n\}$ will be denoted by $(j)\sigma$.

We also consider the groupoid $\mathbf{PR}_n^c(K)$ that has as objects permutation representations of a fixed group K ; that is, a group homomorphism $\alpha: K \rightarrow S_n$. Given two permutation representations $\alpha: K \rightarrow S_n, \beta: K \rightarrow S_n$, a morphism from α to β is given by a bijection $\varphi: \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$ such that the following diagram is commutative:

$$\begin{array}{ccc} K & \xrightarrow{\alpha} & S_n \\ \text{id} \downarrow & & \downarrow (\cdot)^\varphi \\ K & \xrightarrow{\beta} & S_n \end{array}$$

where $\sigma^\varphi = \varphi^{-1}\sigma\varphi$, with $\sigma \in S_n$. Note that the product is expressed from left to right.

A permutation representation $\alpha: K \rightarrow S_n$ is said to be transitive if given $a, a' \in \{1, 2, \dots, n\}$, then there is $g \in K$ such that $(a)\alpha(g) = a'$. Note that, given $\alpha: K \rightarrow S_n, \beta: K \rightarrow S_n$, if α is isomorphic to β and α is transitive, then β is also transitive. Denote the corresponding full sub-groupoid of transitive permutation representations by

$$\mathbf{TPR}_n^c(K).$$

Finally, we consider the following notion: We say that a constellation is a v -tuple of permutations $\lambda = (\lambda_1, \dots, \lambda_v) \in S_n^v$ such that $\lambda_1 \cdots \lambda_v = 1$ and such that the subgroup of S_n generated by $\lambda_1, \dots, \lambda_v$ is transitive. For $n, v \in \mathbb{N}$, we denote the set of constellations composed of v permutations by $\text{Const}_n(\leq v)$, or by $\text{Const}_n(v)$ when every permutation is non-trivial. We also define the following subsets:

$$\text{Const}_n^c(\leq v) = \{(\lambda_1, \dots, \lambda_v) \in \text{Const}_n(\leq v) \mid \lambda_v = (1, 2, \dots, n), \sum_{i=1}^{v-1} \delta(\lambda_i) = n-1\},$$

$$\text{Const}_n^c(v) = \{(\lambda_1, \dots, \lambda_v) \in \text{Const}_n^c(\leq v) \mid \delta(\lambda_i) > 0, i \in \{1, \dots, v-1\}\},$$

where $(1, 2, \dots, n)$ denotes the canonical n -cycle and $\delta(\lambda_i) = n - r_i$, where r_i denotes the number of distinct cycles in the k -cycle decomposition (for $k > 1$) of λ_i .

Both sets give rise to the groupoids $\mathbf{Const}_n^c(\leq v), \mathbf{Const}_n^c(v)$ whose objects are the elements of the sets $\text{Const}_n^c(\leq v), \text{Const}_n^c(v)$ respectively, and a morphism from $(\lambda_1, \dots, \lambda_v)$ to $(\lambda'_1, \dots, \lambda'_v)$ is given by a permutation $\varphi \in S_n$ such that $\varphi\lambda'_i = \lambda_i\varphi$ for each $i \in \{1, \dots, v\}$.

Then, the following classification result holds (for all the details, see [1]):

Theorem 1.1. *Suppose that $n > 0$, and consider $V = \{q_1, \dots, q_{v-1}, q_v\} \subset \hat{\mathbb{C}}$ such that $q_v = \infty, v = |V| > 0$. Then, we have that*

- (i) *The functor neb: $\mathbf{BPol}_n(\subset V) \xrightarrow{\phi} \mathbf{TPR}_n^c(K) \xrightarrow{\psi} \mathbf{Const}_n^c(\leq v)$ is an equivalence of groupoids,*
- (ii) *The functor neb: $\mathbf{BPol}_n(V) \xrightarrow{\phi} \mathbf{TPR}_n^c(K) \xrightarrow{\psi} \mathbf{Const}_n^c(v)$ is an equivalence of groupoids,*

where

$$K = \pi_1(\hat{\mathbb{C}} \setminus V, b_0) \cong \langle \bar{\omega}_1, \dots, \bar{\omega}_{v-1}, \bar{\omega}_v \mid \bar{\omega}_1 \cdots \bar{\omega}_{v-1} \bar{\omega}_v = 1 \rangle,$$

denotes the fundamental group of $\hat{\mathbb{C}} \setminus V$, where $\phi(P) := (\lambda_1(P), \dots, \lambda_v(P))$, and $\lambda_i(P) := \lambda(P)(\bar{\omega}_i)(j) = (\tilde{\omega}_i^{(j)\theta_P^{-1}}(1))_{\theta_P}$ where $\tilde{\omega}_i^{(j)\theta_P^{-1}}$ is the unique lift of ω_i starting at $(j)\theta_P^{-1}$ and $j \in \{1, \dots, n\}$, and where, if $\epsilon: K \rightarrow S_n$ is a transitive permutation representation, $\psi(\epsilon) = (\epsilon(\bar{\omega}_1), \dots, \epsilon(\bar{\omega}_{v-1}), \epsilon(\bar{\omega}_v))$.

2. COMBINATORIAL ALGORITHMS AND SHABAT POLYNOMIALS

Following the previous construction, we can implement algorithms able to compute the constellation that the equivalence of groupoids *neb* associates to a polynomial P . Since the groupoids $\mathbf{Const}_n^e(\leq v)$ and $\mathbf{Const}_n^e(v)$ are finite, we can compute a combinatorial classification table for constellations (and thereby, for polynomials), as it can be seen in [1], at least for low values of n and v . A classical example often addressed in the literature is that of $v = 3$; that is, the classification of polynomials with at most 3 critical values (including the infinity point); the so-called Shabat polynomials. Regarding the study and classification of Shabat polynomials, we can consider combinatorial algorithms based on from the presented theory in order to compute the different equivalence classes for reasonable values of n . For instance, the number of different equivalence classes of Shabat polynomials of degree n , for $n = 1, \dots, 10$, has been computed: 1, 2, 3, 6, 10, 28, 63, 190, 546, 1708.

Using these techniques and algorithms, one can also compute the automorphism group of a polynomial P , and derive some of the topological properties of P as a branched cover of the Riemann sphere, such as its regularity.

Moreover, this approach and the algorithms that allow us to compute the classification table can be adapted to different contexts in which they might be of use. For example, a root-finding algorithm based on the lifting of paths on the Riemann sphere can be implemented for an arbitrary polynomial (or even rational) equation. Different algebraic invariants of a polynomial map (such as its monodromy action, monodromy group, or group of automorphisms) can be also obtained and visualized with the implemented methods.

These methods and algorithms have been implemented in Julia Language, and can be found in the GitHub repository *PathLifting.jl* [2].

REFERENCES

- [1] V. Álvarez-Aparicio, L.J. Hernández-Paricio and M.T. Rivas-Rodríguez, *Combinatorial classification of polynomials with critical values in a given finite set*, 2024, Preprint.
- [2] V. Álvarez-Aparicio (2023). *PathLifting.jl*. [Online].
- [3] R.H. Fox, *Covering spaces with singularities*, 1957, A Symposium in honor of S. Lefschetz, 243–257.
- [4] H. Freudenthal, *Über die Enden topologischer Bäume und Gruppen*, 1931, Mathematische Zeitschrift, 33, 692–713.
- [5] Sergei Lando and Alexander Zvonkin, *Graphs on Surfaces and Their Applications*, 01 2004, Encyclopaedia of mathematical sciences, 141.
- [6] George Shabat and Alexander Zvonkin, *Plane trees and algebraic numbers*, 1994, Amer. Math. Soc., Providence, RI.

University of La Rioja

Email address: valvarezaparicio@gmail.com

PROOFS OF APPROXIMATION FORMULAS BASED ON THE CLOSEST TREE ALGORITHM

ERNESTO ÁLVAREZ GONZÁLEZ

ABSTRACT. In the early nineties, Hendy and Penny (1993) developed the two-state closest tree algorithm for estimating the optimal branch lengths of a phylogenetic tree, whose parameters correspond to the Cavender's model of molecular evolution. This procedure also helps to determine the true topology of the phylogenetic tree giving rise to related current species. On the other hand, Steel et al. (1992) developed the four-state version of the closest tree algorithm. In both cases, the authors provide formulas of approximation (without proofs) for computing the optimal values of tree branch lengths. Throughout this manuscript, we contribute with proofs for these formulas.

INTRODUCTION

This manuscript recovers the elements and concepts dealing with two-state DNA entities as in Hendy and Penny (1993)[1], or dealing with four DNA entities as in Steel et al. (1992)[2], in order to reconstruct the ancestral relations among a set of current species. For any given phylogenetic tree, they explain how to assign a length to the tree branches. In both versions, they stick out the operation called Hadamard conjugation that lets get external information (relative frequencies of DNA entities on the leafs) from internal data (branch lengths) and viceversa. Going from external information to internal data is for what authors provide (without proofs) approximation formulas.

1. APPROXIMATION FORMULA FOR THE CAVENDER'S MODEL

This section is based in the article of Hendy and Penny (1993)[1].

For a given phylogenetic tree, T , with n leaves in $N = \{1, 2, \dots, n\}$, we define subsets S_j (called *bipartitions*) of $N' = N \setminus \{n\}$ ($0 \leq j \leq 2^{n-1}$), in agreement to the binary decomposition of index j : if 2^k belongs to that decomposition, then $k + 1 \in S_j$. We use $E(T)$ to represent the set of branches in T .

A 2^{n-1} -dimensional vector of real numbers, $\vec{x} = (x_0, x_1, x_2, \dots, x_{2^{n-1}-1})$, such that x_i refers to the i -th bipartition of N , is called an *spectrum*. A *tree spectrum* is a 2^{n-1} -dimensional vector of real numbers that encodes the phylogenetic tree: if e_i is a branch of T , then $x_i > 0$; if e_j is not present in T , then $x_j = 0$; $x_0 = -\sum_{e_i \in E(T)} x_i$. A square matrix of orthogonal rows, symmetric and invertible, is called a Hadamard matrix. We identify these matrices with letter H .

Proposition 1.1. *Let $\rho = H\vec{s}$, where $\vec{s}$ is the observed spectrum. To each branch e_i of T we associate the probability p_i that the states at its ends differ. Let $q_i = -\frac{1}{2} \ln(1 - 2p_i)$. Let $\vec{q}$ be the tree spectrum associated with T . Then $\rho = \exp(H\vec{q})$.*

The first author has been partially supported by University Complutense of Madrid.

Corollary 1.2. *Suppose that the probabilities p_i govern the generation of two-state sequences of length c for leaves in T , then $\vec{s} = H^{-1}\rho = H^{-1}(\exp(H\vec{q}))$, where the exponential function is applied term by term on the vector $H\vec{q}$.*

The operation $H^{-1}\exp H$ is known as *Hadamard-exponential conjugation*. The inverse operation, $H^{-1}\ln H$, when can be applied to the observed spectrum $\vec{s}$ (where the logarithm function is applied term to term to the vector $H\vec{s}$), is called *Hadamard-log conjugation*. The vector $(H^{-1}\ln H)\vec{s}$ is also known as the *conjugate spectrum*.

Definition 1.3. For a phylogenetic tree T , its *spectral set*, $W(T)$, is the set of all possible tree spectra of T , that is, all vectors $\vec{w}$ whose positive entries match to branches of T , zeroes indicate no branches in T , and whose first coordinate is negative. The *spectral space*, $W(N)$, is the union of all the spectral sets associated with all possible phylogenetic trees based on the set of leaves N .

$W(N)$ is a subset of the hyperplane $W = \{w | \sum_{i=0}^{m-1} w_i = 0\} \subset \mathcal{R}^m$, with $m = 2^{n-1}$. A point $\gamma \in W$ belongs to $W(N)$ if and only if $\gamma_i \geq 0$ for all $i > 0$ and if for every pair of indices i, j taken from N , with $\gamma_i, \gamma_j > 0$, bipartitions S_i and S_j are compatible ($S_i \cap S_j \in \{\emptyset, S_i, S_j\}$). Given a point $\gamma \in W$, we wish to find a point in $W(N)$ closest to γ . The *selection of the closest tree* $(T, \vec{w})$ with $w \in \vec{W}(T)$ is closest to γ , using the Euclidean metric.

Proposition 1.4. (*Approximation formula*) *Let $\gamma \in W$ and let T be a phylogenetic tree with n branches $e \in E(T) = E$. Let $\gamma_T = \frac{1}{n+1}(\gamma_0 + \sum_{e_i \in E} \gamma_i)$. The point closest to γ in the spectral space of T is $w = W(T)$, where $w_i = \gamma_i - \gamma_T$ for all $e_i \in E$ (provided $\gamma_i > \gamma_T$).*

Proof. Let $\gamma' \in W(T)$. We wish to minimize

$$\begin{aligned} \|\gamma' - \gamma\|^2 &= \sum_{e_i \in E} (\gamma'_i - \gamma_i)^2 + \sum_{e_i \notin E} (-\gamma_i)^2 + (-\sum_{e_i \in E} \gamma'_i - \gamma_0)^2 = \\ &= 2 \sum_{e_i \in E} (\gamma'_i)^2 + \sum_{e_i \in E} (\gamma_i)^2 + \sum_{\substack{e_i \notin E \\ i > 0}} (\gamma_i)^2 + \\ &\quad - 2 \sum_{e_i \in E} \gamma'_i \gamma_i + 2 \sum_{\substack{e_i, e_j \in E \\ i \neq j}} \gamma'_i \gamma'_j + 2\gamma_0 \sum_{e_i \in E} \gamma'_i + (\gamma_0)^2. \end{aligned}$$

The system

$$(1) \quad (\partial \|\gamma' - \gamma\|^2 / \partial \gamma'_i = 2\gamma'_i + \sum_{j \neq i} \gamma'_j + \gamma_0 - \gamma_i = 0)_{e_i \in E}$$

is linear in the parameters. □

2. APPROXIMATION FORMULA FOR THE KIMURA'S 3 PARAMETER MODEL

Let $\mathbb{K} = \mathbb{Z}_2 \times \mathbb{Z}_2$ be the Klein group. We denote the nucleotides as $A = (0, 0), G = (0, 1), C = (1, 0), T = (1, 1)$. A sequence of nucleotides at the n leaves L of T is a pair $\theta = (\sigma_1, \sigma_2)$ of subsets of $N = \{1, 2, \dots, n\}$ such that, if π_1 and π_2 are the projections of σ_1 and σ_2 on their first and second coordinates, respectively, then $\sigma_1 = \{k \in L, k \neq R : \pi_1(\chi(k) + \chi(R)) = 1\}$ and $\sigma_2 = \{k \in L, k \neq R : \pi_2(\chi(k) + \chi(R)) = 1\}$. Given an m -tuple associated with an alignment of size n , x_θ is the proportion of sequences of L in correspondence with θ . By sorting the pairs θ , the proportions x_θ 's form a vector x of 4^{n-1} non-negative entries that sum to 1.

Let $H' = ((-1)^{|\sigma \cap \sigma'|})$ be the $2^{n-1} \times 2^{n-1}$ matrix, where $\sigma, \sigma' \subset L$. We compute the kronecker product $H = H' \otimes H'$. Both H' and H are Hadamard matrices. Given $y \in \mathbb{R}^{+k}$ (respectively $y \in \mathbb{R}^k$), we define $\log(y)$ (respectively $\exp(y)$) as the vector whose i -th coordinate is $\log(y_i)$ (respectively $\exp(y_i)$) for $i \in \{1, 2, \dots, k\}$. If $(Hx)_i > 0 \forall i$, we define $\gamma(x) = H^{-1}(\log(Hx^t))$, where super index t means transposition. We call $\gamma(x) = (\gamma_\theta(x))$ the *conjugate spectrum*.

Let f_θ be the probability of observing at each site of the alignment the sequence of nucleotides θ . We calculate f_θ according to the Kimura's 3-parameter model. The state changes are classified in three ways: transitions ($A \leftrightarrow G, T \leftrightarrow C$), type I transversions ($C \leftrightarrow G, T \leftrightarrow A$) and type II ($A \leftrightarrow C, T \leftrightarrow G$).

Let ρ be a branch of T . The expected values of transitions, type I transversions, and type II transversions are denoted by $E_\rho^2, E_\rho^3, E_\rho^1$, respectively. Let's set $\mathcal{C}(T) = \{(0, 0)\} \cup \{\rho^{(i)} : \rho \in T, i = 1, 2, 3\}$, where $\rho^1 = (\rho, \emptyset)$, $\rho^2 = (\emptyset, \rho)$, $\rho^3 = (\rho, \rho)$. Let $\gamma_\rho = \gamma_\rho(\mathbf{x})$ and take $\gamma_T = \sum_{\theta \in \mathcal{C}(T)} \gamma_\theta$.

Theorem 2.1. *Given a distribution $f = f(T, P)$ for the sequences on the leaves of T , whose molecular evolution model is Kimura's 3 parameter, we have the following:*

$$\gamma_\theta(f) = \begin{cases} 0, & \text{if } \theta \notin \mathcal{C}(T), \\ E_\rho^i, & \text{if } \theta = \rho^{(i)}, \rho \in T, \\ -\sum_{\rho \in T} \mathbf{j} \cdot \mathbf{E}_\rho, & \text{if } \theta = (\emptyset, \emptyset). \end{cases}$$

If $\mathbf{x}_\theta$ is the relative frequency of θ over observed sequences, we can propose $(\mathbf{x}_\theta)$ as an estimate of $f(T')$ with T' unknown. For each tree topology T , we can search the Kimura's 3 parameters by minimizing the Euclidean distance $D(T, \mathbf{x}) = \|\gamma(x) - \gamma(f(T))\|$. A *closest tree* for $\mathbf{x}$ is a tree T that minimizes $D(T, \mathbf{x})$.

Corollary 2.2. *(Approximation formula)*

For all phylogenetic tree T , the values for E_ρ^i minimizing $D(T, \mathbf{x})$ are given by

$$(2) \quad E_\rho^i = \gamma_{\rho^{(i)}} - \frac{1}{c} \gamma_T,$$

with $c = 3|T| + 1$.

Proof. We wish to minimize

$$\begin{aligned}
& \|D(T, x)\|^2 = \\
& \|\gamma(x) - \gamma(f(T, P))\|^2 = \sum_{(\sigma_1, \sigma_2)} \{[H^{-1}(\log(Hx^t))]_{(\sigma_1, \sigma_2)} - \gamma_{(\sigma_1, \sigma_2)}(f)\}^2 = \\
& \sum_{(\emptyset, \sigma)} [H^{-1}(\log(Hx^t))_{(\emptyset, \sigma)} - E_{(\emptyset, \sigma)}^2]^2 + \sum_{(\sigma, \emptyset)} [H^{-1}(\log(Hx^t))_{(\sigma, \emptyset)} - E_{(\sigma, \emptyset)}^1]^2 + \\
& \sum_{(\sigma, \sigma)} [H^{-1}(\log(Hx^t))_{(\sigma, \sigma)} - E_{(\sigma, \sigma)}^3]^2 + [H^{-1}(\log(Hx^t))_{(\emptyset, \emptyset)} - \gamma_{(\emptyset, \emptyset)}(f)]^2 + \\
& \sum_{(\sigma, \sigma') \notin \mathcal{C}(T)} [H^{-1}(\log(Hx^t))_{(\sigma, \sigma')}]^2 = \\
& \sum_{(\emptyset, \sigma)} \{[H^{-1}(\log(Hx^t))]_{(\emptyset, \sigma)}^2 - 2[H^{-1}(\log(Hx^t))]_{(\emptyset, \sigma)} E_{(\emptyset, \sigma)}^2 + [E_{(\emptyset, \sigma)}^2]^2\} + \\
& \sum_{(\sigma, \emptyset)} \{[H^{-1}(\log(Hx^t))]_{(\sigma, \emptyset)}^2 - 2[H^{-1}(\log(Hx^t))]_{(\sigma, \emptyset)} E_{(\sigma, \emptyset)}^1 + [E_{(\sigma, \emptyset)}^1]^2\} + \\
& \sum_{(\sigma, \sigma)} \{[H^{-1}(\log(Hx^t))]_{(\sigma, \sigma)}^2 - 2[H^{-1}(\log(Hx^t))]_{(\sigma, \sigma)} E_{(\sigma, \sigma)}^3 + [E_{(\sigma, \sigma)}^3]^2\} + \\
& [H^{-1}(\log(Hx^t))]_{(\emptyset, \emptyset)}^2 - 2[H^{-1}(\log(Hx^t))]_{(\emptyset, \emptyset)} \gamma_{(\emptyset, \emptyset)}(f) + [\gamma_{(\emptyset, \emptyset)}(f)]^2 + \\
& \sum_{(\sigma, \sigma') \notin \mathcal{C}(T)} [H^{-1}(\log(Hx^t))]_{(\sigma, \sigma')}^2.
\end{aligned}$$

Let's calculate the critical points of the function $\|D(T, x)\|^2$, partially differentiating with respect to each of the variables $E_{\rho(j)}$ ($\rho(j) \in \mathcal{C}(T), j \in \{1, 2, 3\}$) and equal to zero. This leads to the system of linear equations

$$\begin{aligned}
& (\partial \|D(T, x)\|^2 / \partial E_{\rho(j)}^j = -2[H^{-1}(\log(Hx^t))]_{\rho(j)} + 2E_{\rho(j)}^j + 2[H^{-1}(\log(Hx^t))]_{\emptyset, \emptyset} \\
& + 2E_{\rho(j)}^j + 2 \sum_{\rho'(j) \neq \rho(j)} E_{\rho'(j)}^j + 2 \sum_{\substack{\rho'(i) \\ i \neq j}} E_{\rho'(i)}^i + 2 \sum_{\substack{\rho'(k) \\ k \neq j}} E_{\rho'(k)}^k = 0)_{\substack{\rho(j) \in \mathcal{C}(T) \\ j \in \{1, 2, 3\}}},
\end{aligned}$$

where $\{i, j, k\} = \{1, 2, 3\}$.

□

REFERENCES

- [1] M.D. Hendy, and David Penny, *Spectral Analysis of Phylogenetic Data*, Journal of Classification. **10** 5-24 (1993). doi: 10.1007/BF02638451
- [2] M.A. Steel and M.D. Hendy and L.A. Székely and P.L. Erdős, *Spectral analysis and a closest tree method for genetic sequences*, Appl. Math. Lett. **5**(6) 63-67 (1992). doi: 10.1016/0893-9659(92)90016-3

Complutense University of Madrid ...
 Email address: eralva01@ucm.es

ON THE SENSITIVITY OF TRILEAN FUNCTIONS

SARA ASENSIO, IGNACIO GARCÍA-MARCO, AND KOLJA KNAUER

ABSTRACT. The study of the relations between different complexity measures of boolean functions led Nisan and Szegedy to state the sensitivity conjecture in 1994. This problem remained unsolved until 2019, when Huang proved the conjecture by means of an equivalent reformulation of the problem in graph theory. We wonder if the same type of results hold for functions defined on finite alphabets of cardinality greater than two. This work concerns functions over an alphabet with three symbols, which we call *trilean functions*. In this context we follow the steps of Nisan and Szegedy and extend most of the results for boolean functions. Also, we find an equivalent reformulation in graph theoretical terms of the trilean version of the sensitivity conjecture.

INTRODUCTION

One can measure how complex a given boolean function $f : \{0, 1\}^n \rightarrow \{0, 1\}$ is in many ways, and these different conceptions give rise to different complexity measures such as: the degree, the sensitivity, the block sensitivity, the decision tree complexity... In 1994, it was already known that all these complexity measures were polynomially related except the sensitivity. This led Nisan and Szegedy to the statement of the sensitivity conjecture [5], which claimed that the sensitivity was also polynomially related to the other measures. This conjecture was proved almost 30 years later by Huang [4], and his proof relies on an equivalence theorem due to Gotsman and Linial [3] which translated the sensitivity conjecture to an equivalent problem in graph theory. An extended summary of this story can be found in [1].

After this study, it is natural to ask whether there is a similar situation with functions $f : T^m \rightarrow T$, where T is a finite set of cardinality $m > 2$. Our work focuses on the case $m = 3$ and its corresponding functions, which we call *trilean functions*. For technical reasons, our set T will be the set $\{1, \varepsilon, \varepsilon^2\}$ where ε is a primitive cubic root of unity.

This abstract is divided in four sections. In the first one, we define two complexity measures of a trilean function f , namely the sensitivity $s(f)$ and the degree $\deg(f)$. In Proposition 1.4 we provide a quadratic upper bound for the sensitivity in terms of the degree. This was also known for boolean functions before 1994. Again, the most difficult question seems to be the construction of a polynomial bound in the other direction. In the second section we prove in Theorem 2.2 that providing an upper bound for the degree in terms of the sensitivity is equivalent to a graph theoretical problem that can be entirely stated in terms of a generalization of the n -dimensional hypercube. In the third section, by means of

All the authors have been partially supported by the Spanish MICINN through grant PID2022-137283NB-C22, and also by the “European Union NextGenerationEU/PRTR” through grant TED2021-130358B-I00 in the case of the first author.

The talk at the meeting EACA 2024 has been given by the first author.

Theorem 2.2 we show that there are trilean functions such that $s(f) < \sqrt{2 \deg(f)} + 1$. We conclude with a future work section.

1. TWO COMPLEXITY MEASURES AND THE FIRST RELATION BETWEEN THEM

First of all, let's define two complexity measures of trilean functions which generalize those of boolean functions. The first one is the degree, whose definition relies on the following result:

Proposition 1.1. *Let $f : \{1, \varepsilon, \varepsilon^2\}^n \rightarrow \{1, \varepsilon, \varepsilon^2\}$ be a trilean function. Then, there is a unique polynomial $F \in \mathbb{C}[x_1, \dots, x_n]$ of degree at most 2 in each variable that represents f (i.e., $F(\mathbf{x}) = f(\mathbf{x})$ at every $\mathbf{x} \in \{1, \varepsilon, \varepsilon^2\}^n$).*

Definition 1.2. The *degree* of a trilean function $f : \{1, \varepsilon, \varepsilon^2\}^n \rightarrow \{1, \varepsilon, \varepsilon^2\}$ is the degree of the unique polynomial of degree at most 2 in each variable that represents f .

The second complexity measure of trilean functions we are considering is the sensitivity.

Definition 1.3. The *local sensitivity* of a trilean function f at $\mathbf{x} \in \{1, \varepsilon, \varepsilon^2\}^n$, $s_{\mathbf{x}}(f)$, is the number of elements $\mathbf{y} \in \{1, \varepsilon, \varepsilon^2\}^n$ which differ from $\mathbf{x}$ in exactly one entry and $f(\mathbf{x}) \neq f(\mathbf{y})$.

The *sensitivity* of f is $s(f) = \max_{\mathbf{x} \in \{1, \varepsilon, \varepsilon^2\}^n} \{s_{\mathbf{x}}(f)\}$.

We have the following polynomial upper bound for the sensitivity of a trilean function in terms of its degree:

Proposition 1.4. *For every trilean function $f : \{1, \varepsilon, \varepsilon^2\}^n \rightarrow \{1, \varepsilon, \varepsilon^2\}$, $s(f) \leq 64 \deg(f)^2$.*

2. THE EQUIVALENCE THEOREM

The proof of the sensitivity conjecture for boolean functions would not have been possible without the equivalence theorem by Gotsman and Linial [3], which stated that solving the sensitivity conjecture was equivalent to solving a combinatorial problem in graph theory. That problem consisted on finding a polynomial lower bound on n for the maximum between the maximum degree of every induced subgraph of the n -dimensional hypercube with not exactly half of its vertices and the maximum degree of its complementary.

We have obtained an equivalence theorem in the trilean case, which is somehow more involved than the boolean one. Before presenting its statement, we need to introduce some definitions and notation.

In the case of boolean functions, the set $\{0, 1\}^n$ where they are defined can be seen as the vertex set of the n -dimensional hypercube Q_n . In the context of trilean functions, a natural generalization is the graph G whose vertex set is $\{1, \varepsilon, \varepsilon^2\}^n$ and where two vertices are adjacent if and only if they differ in exactly one of their entries. This graph can be described in terms of the cartesian product of graphs:

Definition 2.1. Given two graphs G and H , its *cartesian product* $G \square H$ is the graph with vertex set $V(G) \times V(H)$ and whose edges are the pairs $\{(u, v), (u', v')\}$ such that

- $u = u'$ and $\{v, v'\}$ is an edge of H , or
- $v = v'$ and $\{u, u'\}$ is an edge of G .

If we denote the complete graph on three vertices (the triangle graph) by Δ , then the generalization of the n -dimensional hypercube in the above sense is the graph $\Delta \square \dots \square \Delta = \Delta^{\square n}$. We observe that the product of the entries of every vertex provides a proper 3-coloring of $\Delta^{\square n}$ (see Figure 1 for a 3-coloring of $\Delta^{\square 2}$).

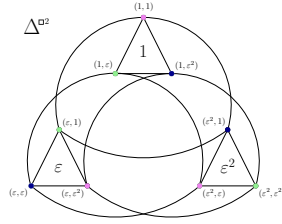


FIGURE 1. A proper 3-coloring of $\Delta^{\square 2}$.

We are going to denote each set of the resulting tripartition by C_i with $i \in \{1, \varepsilon, \varepsilon^2\}$; i.e.,

$$C_i = \left\{ \mathbf{x} = (x_1, \dots, x_n) \in \{1, \varepsilon, \varepsilon^2\}^n \mid \prod_{j=1}^n x_j = i \right\}.$$

Furthermore, given three induced subgraphs $H_1, H_\varepsilon, H_{\varepsilon^2}$ of $\Delta^{\square n}$ whose vertex sets constitute a tripartition of $\{1, \varepsilon, \varepsilon^2\}^n$, we define three new induced subgraphs (see Figure 2):

- H'_1 , with $V(H'_1) = (V(H_1) \cap C_1) \cup (V(H_{\varepsilon^2}) \cap C_\varepsilon) \cup (V(H_\varepsilon) \cap C_{\varepsilon^2})$.
- H'_ε , with $V(H'_\varepsilon) = (V(H_\varepsilon) \cap C_1) \cup (V(H_1) \cap C_\varepsilon) \cup (V(H_{\varepsilon^2}) \cap C_{\varepsilon^2})$.
- H'_{ε^2} , with $V(H'_{\varepsilon^2}) = (V(H_{\varepsilon^2}) \cap C_1) \cup (V(H_\varepsilon) \cap C_\varepsilon) \cup (V(H_1) \cap C_{\varepsilon^2})$.

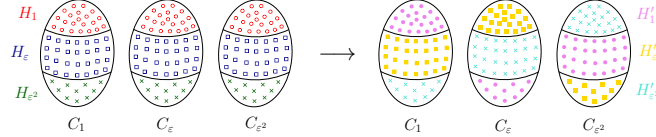


FIGURE 2. The vertices of $H'_1, H'_\varepsilon, H'_{\varepsilon^2}$ can be visualized as a certain cyclic rotation of the vertices of $H_1, H_\varepsilon, H_{\varepsilon^2}$.

Theorem 2.2 (Equivalence theorem). *The following are equivalent for any function $h : \mathbb{N} \rightarrow \mathbb{R}$:*

- (1) *For any induced subgraphs H_1, H_ε and H_{ε^2} of $\Delta^{\square n}$ such that their vertex sets constitute a tripartition of $V(\Delta^{\square n})$ and the corresponding H'_1, H'_ε and H'_{ε^2} do not verify that $|V(H'_1)| = |V(H'_\varepsilon)| = |V(H'_{\varepsilon^2})| = 3^{n-1}$,*

$$\Gamma(H_1, H_\varepsilon, H_{\varepsilon^2}) = 2n - \min\{\delta(H_1), \delta(H_\varepsilon), \delta(H_{\varepsilon^2})\} \geq h(n),$$

where $\delta(H_i)$ is the minimum degree of H_i for all $i \in \{1, \varepsilon, \varepsilon^2\}$.

- (2) *For any trilean function $f : \{1, \varepsilon, \varepsilon^2\}^n \rightarrow \{1, \varepsilon, \varepsilon^2\}$, $s(f) \geq h(\frac{1}{2} \deg(f))$.*

Hence, if we could prove the first statement for a polynomial function h , we would have proved the sensitivity conjecture in the trilean case.

3. SEARCHING FOR TRILEAN FUNCTIONS WITH LOW SENSITIVITY AND HIGH DEGREE

In the case of boolean functions, Chung, Füredi, Graham and Seymour [2] proved that there exists an induced subgraph of the n -dimensional hypercube with $2^{n-1} + 1$ vertices whose maximum degree is strictly smaller than $\sqrt{n} + 1$. By Gotsmann-Linial's equivalence theorem, this resulted in the existence of boolean functions with $s(f) < \sqrt{\deg(f)} + 1$. Interestingly, Huang later proved that $s(f) \geq \sqrt{\deg(f)}$ for every boolean function f .

In the trilean case, we have proved that there are three induced subgraphs H_1 , H_ε and H_{ε^2} of $\Delta^{\square n}$ such that

- their vertices constitute a tripartition of $\{1, \varepsilon, \varepsilon^2\}^n$,
- the corresponding H'_1 , H'_ε and H'_{ε^2} do not verify that $|V(H'_1)| = |V(H'_\varepsilon)| = |V(H'_{\varepsilon^2})| = 3^{n-1}$, and
- $\Gamma(H_1, H_\varepsilon, H_{\varepsilon^2}) = 2n - \min\{\delta(H_1), \delta(H_\varepsilon), \delta(H_{\varepsilon^2})\} < 2\sqrt{n} + 1$.

This construction together with Theorem 2.2 yields the following:

Proposition 3.1. *There exist trilean functions $f : \{1, \varepsilon, \varepsilon^2\}^n \rightarrow \{1, \varepsilon, \varepsilon^2\}$ such that*

$$s(f) < \sqrt{2\deg(f)} + 1.$$

4. FUTURE WORK

The main open problem now is to determine whether the sensitivity conjecture is true or not in the trilean case, which is essentially a combinatorial problem in graph theory thanks to the equivalence theorem. Furthermore, it would be interesting to generalize all of our results to the case of functions on finite sets of cardinality greater than three.

REFERENCES

- [1] S. Asensio, 2023: La conjetura de la sensibilidad y su resolución vía teoría de grafos, *La Gaceta de la RSME*, **26**(1), 131-148.
- [2] F. R. K. Chung, Z. Füredi, R. L. Graham and P. Seymour, 1988: On induced subgraphs of the cube, *J. Combin. Theory Ser. A*, **49**, 180-187, [https://doi.org/10.1016/0097-3165\(88\)90034-9](https://doi.org/10.1016/0097-3165(88)90034-9).
- [3] C. Gotsman and N. Linial, 1992: The equivalence of two problems on the cube, *J. Combin. Theory Ser. A*, **61**, 142-146, [https://doi.org/10.1016/0097-3165\(92\)90060-8](https://doi.org/10.1016/0097-3165(92)90060-8).
- [4] H. Huang, 2019: Induced subgraphs of hypercubes and a proof of the sensitivity conjecture, *Ann. of Math.*, **190**(3), 949-955, <https://doi.org/10.4007/annals.2019.190.3.6>.
- [5] N. Nisan and M. Szegedy, 1994: On the degree of Boolean functions as real polynomials, *Comput. Complexity*, **4**, 301-313, <https://doi.org/10.1007/BF01263419>.

Instituto de Investigación en Matemáticas de la Universidad de Valladolid (IMUVa), Universidad de Valladolid

Email address: sara.asensio@uva.es

Instituto de Matemáticas y Aplicaciones (IMAULL), Universidad de La Laguna

Email address: iggarcia@ull.edu.es

Universitat de Barcelona

Email address: kolja.knauer@gmail.com

MULTIGRADED CASTELNUOVO-MUMFORD REGULARITY AND GRÖBNER BASES

MATÍAS BENDER, LAURENT BUSÉ, CARLES CHECA, AND ELIAS TSIGARIDAS

ABSTRACT. We explore the relation between the multigraded Castelnuovo-Mumford regularity of a multihomogeneous ideal I and the multidegrees of a Gröbner basis of I with respect to the degree reverse lexicographical monomial order in generic coordinates. We introduce a subset of multidegrees that allows us to extend the classical criterion of Bayer and Stillman to the multihomogeneous setting. We also show that (up to a certain shift) the multigraded Castelnuovo-Mumford regularity bounds the multidegrees involved in the computation of these Gröbner bases. Unlike the single graded case, this description does not bound the multidegrees involved in the Gröbner basis computation in a tight manner. We compare our description with some other bounding regions that have been studied in the literature.

Let $\mathbf{k}$ be an infinite field and $S = \mathbf{k}[x_0, \dots, x_n]$ a standard $\mathbb{Z}$ -graded polynomial ring. Consider a homogeneous polynomial ideal $I \subset S$. A widely used method to perform many algebraic operations (eliminate variables, compute minimal free resolutions...) is to employ Gröbner bases. This consists of fixing a monomial order on S and finding generators of the *initial ideal*, i.e.

$$\text{in}(I) = (\text{in}(f) \mid f \in I)$$

where the *initial term* $\text{in}(f)$ is the highest term of f with respect to the monomial order. A set of generators of I whose initial terms generate $\text{in}(I)$ is known as a *Gröbner basis* and it is *minimal* if its initial terms are a minimal set of generators of $\text{in}(I)$.

As the graded structure is closely attached to the ideal I , it is common to consider the maximal degree of the generators of $\text{in}(I)$ as an effective measure of the complexity associated with the algebraic operations that use Gröbner bases. In this context, the Castelnuovo-Mumford regularity emerges as a bound for this degree.

The ideal I is called m -regular if the degrees of its j -th syzygies (Betti numbers) are bounded above by $m + j$. The Castelnuovo-Mumford regularity $\text{reg}(I)$ is the minimal m such that I is m -regular. From the point of view of commutative algebra, this invariant also reflects many interesting properties of I , through its relation with local cohomology modules. As it bounds the Betti numbers, the regularity of the initial ideal bounds the degrees at which $\text{in}(I)$ is generated. Therefore, the maximal degree of the elements of a minimal Gröbner basis is bounded above by $\text{reg}(\text{in}(I))$. A relation between the computations made with I and its initial ideal arises by noticing that

$$\text{reg}(I) \leq \text{reg}(\text{in}(I)).$$

The work will be presented by Carles Checa. This project has received funding from the European Union's Horizon 2020 research and innovation programme under the MSC grant agreement No 860843.

Computations in degrees higher than $\text{reg}(I)$ might be redundant, which leads to the question of how to avoid the calculations in these degrees. The work of Bayer and Stillman [2] provided a very relevant answer. Namely, they showed that: *i*) choosing the degree reverse lexicographical monomial order, which we will denote as DRL, can lead to lowering the degrees involved in the computations and *ii*) considering a generic linear change of coordinates in the ideal is also recommended. In other words, one should compute with the generic initial ideal $\text{gin}(I)$, instead of $\text{in}(I)$.

Most computer algebra systems incorporate these two concepts. The algebraic explanation for the answer of Bayer and Stillman follows from the fact that, under these two assumptions, the complexity of Gröbner bases relies solely on the Castelnuovo-Mumford regularity of I , and not of its initial ideal. Namely, under the assumption of using the DRL monomial order and I being in generic coordinates, they proved the equalities

$$(1) \quad \max\{\text{degrees of the elements in a minimal Gröbner basis}\} = \text{reg}(\text{gin}(I)) = \text{reg}(I).$$

Therefore, the Castelnuovo-Mumford regularity describes tightly the complexity of computing with Gröbner bases.

Multihomogeneous polynomial systems. The polynomial systems that arise in many applications have further structure that one might try to exploit for the better design of algorithms and the understanding of the algebraic properties of the ideals. A first (and more simple) case of interest are multihomogeneous polynomial systems, this is, systems where a multidegree is prescribed in several groups of variables.

The multigraded Castelnuovo-Mumford regularity has attracted the interest of many researchers in the last decades. However, the need of a multigraded generalization of the Bayer and Stillman criterion that uses the multidegrees that generate the Gröbner basis has remained an open problem. For the sake of simplicity, we will describe our results in the bigraded case i.e., when the degrees are prescribed in two groups of variables, that we will denote with x 's and y 's. All the discussion and results that follow extend to the multigraded setting.

Let $S = \mathbf{k}[x_0, \dots, x_n, y_0, \dots, y_m]$ be (standard) $\mathbb{Z}^2$ -graded ring with $\deg(x_i) = (1, 0)$ and $\deg(y_j) = (0, 1)$ i.e. S is the coordinate ring of the product of two projective spaces $\mathbb{P}^n \times \mathbb{P}^m$. Let $\mathfrak{m}_x$ (resp. $\mathfrak{m}_y$) be the ideal generated by $x_0, \dots, x_n$ (resp. $y_0, \dots, y_m$) and let $\mathfrak{b} = \mathfrak{m}_x \mathfrak{m}_y$ be the irrelevant ideal of $\mathbb{P}^n \times \mathbb{P}^m$.

The computational advantages of using the DRL monomial order are maintained in this case. However, the relative order of the variables of different bi-degrees becomes a relevant choice to make. We choose an order of the variables in the DRL order such that:

$$(2) \quad x_0 < \dots < x_n < y_0 < \dots < y_m.$$

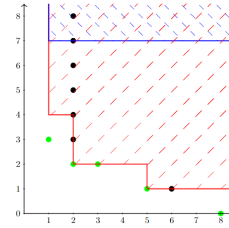
On the other hand, the generic linear change of coordinates that we can consider must preserve the bigraded structure, leading to the bigeneric initial ideal $\text{bigin}(I)$, which still depends on the relative order of the variables of different bi-degrees.

A generalization of the Castelnuovo-Mumford regularity to the bigraded setting, which we also denote as $\text{reg}(I)$, was given by Maclagan and Smith in [6], by using local cohomology modules with respect to $\mathfrak{b}$.

Definition 0.1. Consider a bihomogeneous ideal $I \subset S$. The bigraded Castelnuovo-Mumford regularity $\text{reg}(I)$ is the subset of $\mathbb{Z}^2$ formed by the bi-degrees (a, b) that satisfy $H_{\mathfrak{b}}^i(I)_{(a', b')} = 0$ for $i \geq 1$ and for all $(a', b') \geq (a - \lambda_x, b - \lambda_y)$ where $\lambda_x, \lambda_y \in \mathbb{Z}_{\geq 0}$ satisfy $\lambda_x + \lambda_y = i - 1$. Here, $H_{\mathfrak{b}}^i(I)_{(a', b')}$ denotes the graded part of bidegree (a', b') of the local cohomology of I with respect to $\mathfrak{b}$.

This definition preserves some of the most relevant geometric properties of the classical Castelnuovo-Mumford regularity. The work that we summarize in this *extended abstract* aims to establish a connection between this extension of the Castelnuovo-Mumford regularity and the degrees of the minimal generators of the DRL Gröbner basis after a generic change of coordinates that preserves the bigraded structure.

Using the Hilbert function, it is possible to establish a first link in the case that the ideal I defines an empty scheme. However, we can also show with an example, the difficulty of establishing a general connection as the one in (1). Building upon ideas appearing in the works of Botbol, Chardin and Holanda [3, 5], we can see that considering the local cohomology modules with respect to the ideals generated by each group of variables can also be very advantageous. In this direction, we introduce a subset of bidegrees $\text{x-reg}(I)$ which depends solely on the local cohomology with respect to one group of variables.



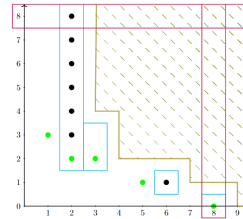
The green dots represent the bi-degrees (a, b) of the generators of I and the black dots represent the bi-degrees (a, b) of new minimal generators of $\text{bigin}(I)$. Moreover, we mark in red the region $\text{reg}(I)$ and in blue the contour of the region $\text{reg}(\text{bigin}(I))$. The ideal is an adaptation of [4, Example 4.3]

Definition 0.2. Let $I \subset S$ be a bihomogeneous ideal. We denote by $\text{x-reg}(I)$ the region of bi-degrees $(a, b) \in \mathbb{Z}^2$ satisfying $H_{\mathfrak{m}_x}^i(I)_{(a', b')} = 0$ for all $i \geq 1$ and $(a', b') \geq (a - i + 1, b)$.

With $\text{x-reg}(I)$ as the pivot of our construction, we prove the following theorem.

Theorem 0.3. Let $I \subset S$ be a bihomogeneous ideal. Then, for every $(a, b) \in \text{reg}(I)$ such that $a > 0$ and $(a', b') \geq (a + n + 1, b)$, there is no generator of $\text{bigin}(I)$ of degree (a', b') .

The shift by $n + 1$ in the first component of the bi-degrees appearing in this theorem can be sharpened in terms of the cohomological dimension of I with respect to $\mathfrak{m}_x$. The structure of the proof can be divided into four steps: first, we relate $\text{reg}(I)$ and $\text{x-reg}(I)$ by using the study of the supports of the local cohomology modules provided by Chardin and Holanda in [5]. Secondly, we give a criterion for describing the bi-degrees in $\text{x-reg}(I)$ in a similar way to the classical results of Bayer and Stillman. Next, we



Using our results, we cannot find generators of $\text{bigin}(I)$ whose degrees lie in the regions $\text{x-reg}(I) + (1, 0)$, which is marked in brown. In the squares and (unbounded) columns in cyan, we can guarantee that there are minimal generators of $\text{bigin}(I)$ of some of those bi-degrees. In purple, we marked the bounds provided in [1, 7].

show that $\text{x-reg}(I)$ behaves well under considering the bigeneric initial ideal if we use the order in (2), i.e.

$$\text{x-reg}(I) = \text{x-reg}(\text{bigin}(I)).$$

Finally, we show that this last result can be used to certify that there are no generators of $\text{bigin}(I)$ of certain bidegrees. In general, the description given by $\text{x-reg}(I)$ will be more accurate than the one given by $\text{reg}(I)$ so we highlight the importance of the region we are introducing.

The question of describing the degrees involved in the generators of $\text{bigin}(I)$ in terms of a bigraded extension of the Castelnuovo-Mumford regularity had already been raised by Aramova, Crona and De Negri in [1] and by Römer in [7]. We compare our description in terms of $\text{x-reg}(I)$ with the one given by Römer and show that $\text{x-reg}(I)$ can also be used to certify the presence of generators of some bi-degrees (both things can be seen in the figures).

REFERENCES

- [1] Annetta Aramova, Kristina Crona, and Emanuela De Negri. “Bigeneric initial ideals, diagonal subalgebras and bigraded Hilbert functions”. In: *Journal of Pure and Applied Algebra* 150.3 (2000), pp. 215–235.
- [2] David Bayer and Michael Stillman. “A criterion for detecting m-regularity”. en. In: *Inventiones Mathematicae* 87.1 (1987), pp. 1–11. ISSN: 0020-9910, 1432-1297. DOI: 10.1007/BF01389151.
- [3] Nicolás Botbol and Marc Chardin. “Castelnuovo Mumford regularity with respect to multigraded ideals”. In: *Journal of Algebra* 474 (2017), pp. 361–392. ISSN: 0021-8693. DOI: <https://doi.org/10.1016/j.jalgebra.2016.11.017>.
- [4] Juliette Bruce, Lauren Cranton Heller, and Mahrud Sayrafi. *Characterizing Multigraded Regularity on Products of Projective Spaces*. 2021. DOI: 10.48550/ARXIV.2110.10705.
- [5] Marc Chardin and Rafael Holanda. *Multigraded Tor and local cohomology*. 2022. DOI: 10.48550/ARXIV.2211.14357.
- [6] Diane Maclagan and Gregory G. Smith. “Multigraded Castelnuovo-Mumford regularity”. In: *Journal für die reine und angewandte Mathematik* 2004.571 (2004), pp. 179–212. DOI: [doi:10.1515/crll.2004.040](https://doi.org/10.1515/crll.2004.040).
- [7] Tim Römer. “Homological properties of bigraded algebras”. In: *Illinois Journal of Mathematics* 45.4 (2001), pp. 1361–1376. DOI: 10.1215/ijm/1258138072.

INRIA AND CMAP, CNRS, INSTITUTE POLYTECHNIQUE DE PARIS, PALAISEAU, FRANCE.
Email address: matias.bender@inria.fr

INRIA CENTRE AT UNIVERSITÉ CÔTE D’AZUR SOPHIA ANTIPOLIS, FRANCE.
Email address: laurent.buse@inria.fr

DEPT. OF INFORMATICS & TELECOMS, NKU ATHENS, ATHENA RC, ATHENS, GREECE.
Email address: ccheca@di.uoa.gr

INRIA AND INSTITUT DE MATHÉMATIQUES DE JUSSIEU SORBONNE UNIVERSITÉ CAMPUS PIERRE ET MARIE CURIE PARIS, FRANCE.
Email address: elias.tsigaridas@inria.fr

OVERVIEW AND EXTENSION OF ROOT-BASED ATTACKS AGAINST PLWE INSTANCES

IVÁN BLANCO CHACÓN, RAÚL DURÁN DÍAZ, AND RODRIGO MARTÍN SÁNCHEZ-LEDESMA

ABSTRACT. The Polynomial Learning With Errors problem (PLWE) serves as background for two of the four cryptosystems standardized in July 2022 by the National Institute of Standards and Technology (NIST) to replace quantum vulnerable current primitives like those based on RSA, finite field based Diffie-Hellman and its elliptic curve analogue. Although PLWE is highly believed to be quantum resistant, unlike other post-quantum proposals like multivariate and some code based ones, this fact has not yet been established. Moreover, several vulnerabilities have been encountered for a number of specific instances. In a search for more flexibility, it becomes fully relevant to study the robustness of PLWE based on other polynomials, not necessarily cyclotomic. In 2015, Lauter et al. found a good number of attacks based on different features of the roots of the polynomial. In this work we present an overview of the approximations made against PLWE derived from these works, along with several new attacks which refine those by Lauter exploiting a) the size of the roots and b) the order of the trace of roots over finite extensions of the finite field.

INTRODUCTION

Let q be a prime and let $f(x) \in \mathbb{Z}[x]$ be a monic irreducible polynomial of degree N . Let $R_q := \mathbb{F}_q[x]/(f(x))$ and choose an element $s(x) \in R_q$. A Polynomial Learning With Errors (PLWE) sample is a pair $(a(x), b(x)) \in R_q^2$ where $a(x)$ is chosen uniformly at random and $b(x) = a(x)s(x) + e(x)$ with the coefficients of $e(x)$ chosen from an R_q -valued random variable of mean 0 and small variance, typically the outcome of discretizing and reducing modulo q the samplings of a centered Gaussian distribution. The set of all possible PLWE samples is referred to as the PLWE distribution and the PLWE problem, in its search version, consists in guessing, with non-negligible advantage, the element $s(x)$ from arbitrarily many samples of the PLWE distribution, while its decision version amounts to be able to distinguish PLWE samples from Uniform ones.

This problem is behind a good number of proposals presented to the NIST competition for standardization of quantum resistant primitives and it is present, in various versions, in several subroutines of three out of the four candidates chosen in July 2022 for KEM and DSA. The PLWE problem as well as its germane problem Ring Learning With Errors

Date: May 11th, 2024.

The first author has been partially supported by MTM2016-79400-P and by grant PID2019-104855RBI00.

The second author has been partially supported by P2QProMeTe (PID2020-112586RB-I00) and by MCIN / AEI / 10.13039 / 501100011033.

The third author has been partially supported by the PQREACT project, funded by a European Union's Horizon Europe Research and Innovation programme, under grant agreement N° 101119547.

The talk at the meeting EACA 2024 has been given by Rodrigo Martín Sánchez-Ledesma.

(RLWE) presents a clear advantage over the Learning With Errors (LWE): the length of the keys necessary to grant (under certain hardness assumptions) the same level of security is essentially linear in N . Other virtues of the cryptosystems based on both R/P-LWE are the ease to implement (specially those based on PLWE) and the fully homomorphic nature of these primitives.

Concerning security, the computational hardness of all the aforementioned problems relies on different versions of the Shortest Vector Problem (over ideal lattices in the case of R/PLWE) which, even if widely believed to be practically unfeasible, should be taken very cautiously over specific instances of the parameters q , N and $f(x)$.

Since 2016, there have appeared different proposals towards the cryptanalysis of specific instances of R/PLWE, all of them assuming that q is totally split in the splitting field of $f(x)$, a condition which even if present in the original reduction of ideal lattice-SVP to RLWE in the cyclotomic setting ([7]), was further proved to be non essential for more general number fields (see for instance [10]).

For instance, in [5] and [6] the authors provide a set of algorithms to break PLWE in its decisional version (and in a good number of cases also in its search version) if the roots of $f(x)$ belong to $\mathbb{F}_q$ and satisfy one of the following conditions:

The first condition is that $\alpha = \pm 1$ is a root of $f(x)$. The second condition is that $f(x)$ has a root of *small* order (typically 3 or 4). These conditions never apply for cyclotomic $f(x)$ but the last two conditions may apply: namely, the third condition is that $f(x)$ has a root of small residue modulo q and the last condition, that the value of certain truncated integral exceeds $1/2$. This condition requires to introduce some technicalities and will be recalled in the next section.

In [2], the authors extend the attacks above to the case where $f(x)$ has a root over a quadratic extension of $\mathbb{F}_q$ of suitable trace and in [1], the authors exploit the splitting behavior of cyclotomic polynomials over finite fields to derive an attack to the restriction of PLWE to a proper subspace of R_q^2 of large enough dimension.

The present work extends our previous results, as well as the last of the attacks of [6], to the setting where $f(x)$ has a root on a higher-degree extension of $\mathbb{F}_q$.

The use of finite field traces for the cryptanalysis of lattice-based primitives is not entirely new (see for instance [8] and [9]). However, to the best of our knowledge, the use we make of the traces of the roots of $f(x)$ is indeed new and the present contribution extends to a more general scenario the methods introduced in [1] and [2].

1. OVERVIEW OF ROOT-BASED ATTACKS AGAINST PLWE SAMPLES

We assume the introduction's setting, taking q such that, initially, $f(x)$ factors completely modulo q . In [5], the authors gave a number of attacks targeting the search and decision versions of PLWE for R_q . These attacks were constructed from a root $\alpha \in \mathbb{F}_q$ of the polynomial $f(x)$ which satisfies certain conditions. Then, the samples are transformed under the evaluation-at- α homomorphism, and distinguished there. Two practical attacks were defined, depending on the strategy followed.

1.1. Attack against the small set of error values. Whenever there exists a root $\alpha \in \mathbb{F}_q$ of $f(x)$ such that the set $S \subset \mathbb{F}_q$ of all polynomials errors $e_i(x)$, evaluated at α , is small enough to be swept through, when compared to $\mathbb{F}_q$.

To construct the attack, we assume that there exists a root $\alpha \in \mathbb{F}_q$ such that it has small order r module q . Then

$$e(\alpha) = \sum_{i=0}^{n-1} e_i \alpha^i = (e_0 + e_r + \dots) + \alpha \cdot (e_1 + e_{r+1} + \dots) + \dots + \alpha^{r-1} \cdot (e_{r-1} + e_{2r-1} + \dots)$$

and thus, if r is small enough, this only generates a handful of possibilities, creating a narrow set S of possibilities which has a cardinal of, at most, $(\frac{4n\sigma}{r})^r$.

With this information, a practical attack can be applied by going through every possible guess g for $s(\alpha) \bmod q$ in $\mathbb{F}_q$ and checking, for each given sample $(a_i(x), b_i(x))$, whether $b_i(\alpha) - a_i(\alpha)g \in S$: if, for any guess g , there is a sample j which does not hold, the guess is discarded. Should a guess verify the condition for every sample, it is considered valid.

Theorem 1.1. [5] *Let S , $|S| < q$ be the set of possible values of $e(\alpha) \bmod q$ and let M be the number of input samples. If the algorithm returns **NOT PLWE**, then the samples come from the uniform distribution, with probability 1. If it outputs anything other than **NOT PLWE**, then the samples are valid PLWE samples with probability $1 - (|S|/q)^M$. In particular, this probability tends to 1 as M grows.*

1.2. Attack against small error values. Whenever there exists a root $\alpha \in \mathbb{F}_q$ of $f(x)$ such that the error polynomials, when evaluated at α , are small themselves.

To construct the attack, we assume that there exists a root $\alpha \in \mathbb{F}_q$ with a certain order r module q . Then $e(\alpha) = \sum_{i=0}^{n-1} e_i \alpha^i$ is a weighted sum of n Gaussians of mean 0 and variance σ^2 , and therefore will be a Gaussian of mean 0 and a certain variance $\bar{\sigma}^2$, dependent upon σ , r and α . Under the assumption that $2\bar{\sigma} < \frac{q}{4}$, every PLWE evaluated error will lie inside $[-\frac{q}{4}, \frac{q}{4}]$.

With this information, a practical attack can be launched in the same fashion as the previous attack, only varying the validation condition, to be $b_i(\alpha) - a_i(\alpha)g \in [-\frac{q}{4}, \frac{q}{4}]$.

Theorem 1.2. [5] *Assume $2\bar{\sigma} < \frac{q}{4}$ and let M be the number of input samples. If the algorithm returns **NOT PLWE**, then the samples come from the uniform distribution, with probability 1. If it outputs anything other than **NOT PLWE**, then the samples are valid PLWE samples with probability $1 - (\frac{1}{2})^M$. In particular, this probability tends to 1 as M grows.*

When $2\bar{\sigma} \geq \frac{q}{4}$, an attack can be launched, if the value

$$P(E_i | D = \mathcal{G}_\sigma) = \left(\int_0^{2\bar{\sigma}} \mathcal{G}_\sigma \right)^{-1} \cdot \left(\int_0^{\frac{q}{4}} \mathcal{G}_\sigma + \sum_{j=0}^{N-1} \int_{\frac{3q}{4}+j\cdot q}^{\frac{5q}{4}+j\cdot q} \mathcal{G}_\sigma \right) > \frac{1}{2}$$

where $N = \frac{2\bar{\sigma}-\frac{q}{2}}{q}$, and E_i is the event of the evaluation, for a guess g of $s(\alpha) \bmod q$, $b_i(\alpha) - ga_i(\alpha)$ to lie inside $[-\frac{q}{4}, \frac{q}{4}]$, creating a *probabilistic* attack.

2. TRACE-BASED GENERALIZATION OF THESE ATTACKS

In a seek for more generality, in [1] and [2], the root α of $f(x)$ is supposed to belong to a proper $\mathbb{F}_q$ -extension of manageable degree. The idea of the attacks presented here is to replace the analysis made over the set of likely values for $e(\alpha) \in \mathbb{F}_q$ by the set of their

$\mathbb{F}_q$ -traces, hence drastically reducing the size of the “smallness set” at the cost of producing just a decisional attack, instead of a search one. This consideration allows generalizing the attack for polynomials $f(x)$ that do not factor completely mod q . For the attack to work the following conditions are required: the existence of an element $a \in \mathbb{F}_q$ such that the polynomial $x^n - a$ divides $f(x)$ in $\mathbb{F}_q[x]$, for $x^n - a$ to be irreducible over $\mathbb{F}_q[x]$, and for a to have small order over $\mathbb{F}_q^*$. In particular, there exists $\alpha \in \mathbb{F}_{q^k}$ such that $\alpha^n - a = 0$ and, therefore, $f(\alpha) = 0$.

Proposition 2.1. *Suppose that $x^n - a$ divides $f(x)$ over $\mathbb{F}_q[x]$ for some $n < N$. Assume that $x^n - a$ is irreducible over $\mathbb{F}_q[x]$ and let $\alpha \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q$ be a root of $f(x)$. Then, for each $j \geq 1$ such that j is not a multiple of n we have that $\text{Tr}(\alpha^j) = 0$.*

With this proposition we have, for each PLWE sample, $(a(x), b(x) = a(x)s(x) + e(x)) \in R_q \times R_q$, setting $s = s(\alpha)$:

$$\text{Tr}(b(\alpha) - a(\alpha) \cdot s) = n \cdot \sum_{i=0}^{r-1} a^i \cdot \sum_{j=0}^{\lfloor \frac{N'}{r} \rfloor - 1} e_{n \cdot (j \cdot r + i)}$$

where r is the multiplicative order of a in $\mathbb{F}_q^*$ and $N' = \lceil \frac{N-1}{n} \rceil$.

This modification can be applied to the previous attacks to elevate them to higher-degree extensions of $\mathbb{F}_q$, by checking $\text{Tr}(b(\alpha) - a(\alpha) \cdot s)$ instead of the sample itself. This comes at the expense of creating just a decisional attack, and increasing the computational complexity of the aforementioned.

To deal with these conditions, the ring $R_{q,0}$ was introduced in [2], as

$$R_{q,0} = \{g(x) \in R_q : g(\alpha) \in \mathbb{F}_q\}.$$

When the samples are taken in $R_{q,0} \times R_q$, we have

$$\text{Tr}(b(\alpha) - a(\alpha)s) = \text{Tr}(b(\alpha)) - a(\alpha)\text{Tr}(s).$$

and therefore the values $\text{Tr}(s)$ can be considered guesses for the trace of $s(\alpha) \bmod q$, while alleviating the overall computational complexity of the attack. This inclusion comes at the expense of requiring samples in $R_{q,0} \times R_q$, with a computational cost on $O(q^{n-1})$, but more feasible than carrying out the attacks over $\mathbb{F}_q^n$. Nevertheless, this cost limits the applicability to extension of degree 3 or 4.

Proposition 2.2. *Assume that $|S| < q$ and let M be the number of input samples. If the Trace-based algorithm for small number of error values returns **NOT PLWE**, then the samples come from the uniform distribution on $R_{q,0} \times R_q$. If it outputs anything other than **NOT PLWE**, then the samples are valid PLWE samples with probability $1 - (|S|/q)^M$. In particular, this probability tends to 1 as M grows.*

Proposition 2.3. *Assume $2\bar{\sigma} < \frac{q}{4}$ and let M be the number of input samples. If the Trace-based algorithm for small error values returns **NOT PLWE**, then the samples come from the uniform distribution. If it outputs anything other than **NOT PLWE**, then the samples are valid PLWE samples with probability $1 - (1/2)^M$. In particular, this probability tends to 1 as M grows.*

REFERENCES

- [1] I. BLANCO-CHACÓN, R. DURÁN-DÍAZ, R. Y. NJAH NCHIWO, AND B. BARBERO-LUCAS, *Trace-based cryptanalysis of cyclotomic $R_{q,0} \times R_q$ -PLWE for the non-split case*, Communications in Mathematics, 31 (2023), pp. 115–135.
- [2] I. BLANCO-CHACÓN, R. DURÁN-DÍAZ, R. Y. NJAH NCHIWO, AND B. BARBERO-LUCAS, *Cryptanalysis of PLWE based on zero-trace quadratic roots*, submitted.
- [3] H. CHEN, K. LAUTER, AND K. E. STANGE, *Attacks on the Search RLWE Problem with Small Errors*, SIAM Journal on Applied Algebra and Geometry, 1 (2017), pp. 665–682.
- [4] L. DUCAS, M. PLANÇON, AND B. WESOŁOWSKI, *On the Shortness of Vectors to Be Found by the Ideal-SVP Quantum Algorithm*, in Advances in Cryptology – CRYPTO 2019, A. Boldyreva and D. Micciancio, eds., vol. 11692, Springer International Publishing, 2019, pp. 322–351.
- [5] Y. ELIAS, K. E. LAUTER, E. OZMAN, AND K. E. STANGE, *Provably Weak Instances of Ring-LWE*, in Advances in Cryptology – CRYPTO 2015, R. Gennaro and M. Robshaw, eds., no. 9215 in Lecture Notes in Computer Science, Berlin, Heidelberg, 2015, Springer Berlin Heidelberg, pp. 63–92.
- [6] ———, *Ring-LWE Cryptography for the Number Theorist*, in Directions in Number Theory, E. E. Eischen, L. Long, R. Pries, and K. E. Stange, eds., vol. 3 of Association for Women in Mathematics Series, Cham, 2016, Springer International Publishing, pp. 271–290.
- [7] V. LYUBASHEVSKY, C. PEIKERT, AND O. REGEV, *On Ideal Lattices and Learning with Errors over Rings*, Journal of the ACM, 60 (2013), pp. 43:1–43:35.
- [8] C. PEIKERT, *How (Not) to Instantiate Ring-LWE*, in Security and Cryptography for Networks, V. Zikas and R. De Prisco, eds., vol. 9841 of Lecture Notes in Computer Science, Springer International Publishing, 2016, pp. 411–430.
- [9] C. PEIKERT AND Z. PEPIN, *Algebraically Structured LWE, Revisited*. Cryptology ePrint Archive, Report 2019/878, 2019. <https://ia.cr/2019/878>.
- [10] M. ROSCA, D. STEHLÉ, AND A. WALLET, *On the Ring-LWE and Polynomial-LWE Problems*, in Advances in Cryptology – EUROCRYPT 2018, J. B. Nielsen and V. Rijmen, eds., Cham, 2018, Springer International Publishing, pp. 146–173.
- [11] K. E. STANGE, *Algebraic Aspects of Solving Ring-LWE, Including Ring-Based Improvements in the Blum–Kalai–Wasserman Algorithm*, SIAM Journal on Applied Algebra and Geometry, 5 (2021), pp. 366–387.
- [12] I. STEWART, D. TALL, *Algebraic number theory and Fermat’s Last Theorem. Third Edition*, A.K. Peters, 2002.

Universidad de Alcalá

Email address: `ivan.blancoc@uah.es`

Universidad de Alcalá

Email address: `raul.duran@uah.es`

Universidad Complutense de Madrid - Indra Sistemas de Comunicaciones Seguras S.A

Email address: `rodrma01@ucm.es`

GEOGEBRA DISCOVERY AND CHATGPT (EXTENDED ABSTRACT)

FRANCISCO BOTANA, TOMÁS RECIO, AND M. PILAR VÉLEZ

ABSTRACT. In our talk we introduce, first the current performance of the programs GeoGebra and GeoGebra Discovery regarding some automatic reasoning tools features for elementary geometry theorems. Then we focus on comparing, through some relevant examples, the performance of ChatGPT and of GeoGebra concerning the same problems. We think that analyzing pros and cons, and developing a cooperation that enhances the best of both approaches is a very relevant and urgent research goal for the next years.

1. THE AUTOMATED GEOMETER IN GEOGEBRA AND GEOGEBRA DISCOVERY: CURRENT PERFORMANCE

GeoGebra (www.geogebra.org) is a freely available software, operative over smartphones, tablets and computers, or just accessible through a web page. It has been translated to circa 100 languages, and is used by more than 100 million persons all over the world, sharing among them over 1 million educational resources. It includes Computer Algebra and Dynamic Geometry features, and can be also used as versatile numerical and statistical calculator. See the above mentioned web for detailed information.

GeoGebra Discovery (see <https://kovzol.github.io/geogebra-discovery/> for further details) includes several off-line releases, for different OS (Mac, Windows, Linux, RaspberryPi, see <https://github.com/kovzol/geogebra/releases>) as well as an on-line version: <https://www.autgeo.online/geogebra-discovery/>. Moreover, GeoGebra Discovery has a specific url for the *Automated Geometer* prototype version (<https://autgeo.online/ag/automated-geometer.html?offline=1>), exclusively devoted to compute all possible statements (following a combinatorial algorithm) that hold true over a given figure.

Along the past decade we have worked towards the development of a kind of *Automated Geometer* ([14, 1, 10, 2, 5, 11, 12]), initially implemented on the popular program GeoGebra and, more recently, extended on GeoGebra Discovery.

For example, GeoGebra is capable of finding an equality relation between two given geometric objects in a construction (i.e. of formulating a thesis holding under the set of hypotheses describing the geometric construction), of checking the truth/failure of a conjectured (by the user) relation, or finding missing hypotheses for a given relation to hold true. And GeoGebra Discovery enlarges GeoGebra tools by including new features (see [5, 6, 11] for details and examples). GeoGebra Discovery is able to find the relation between two given geometric objects in a construction, including, in the case of lengths, the *discovery of relations that are not of equality*: obtaining algebraic number ratios, or

Second and third authors have been partially supported by the grant “Mathematical Visualization: Foundations, Algorithms and Applications” PID2020-113192GB-I00 from the Spanish MICINN.

The talk at the meeting EACA 2024 has been given by second and third authors.

inequality relations, through comparison. It is also capable of checking the truth/failure of a conjectured (by the user) relation *involving inequalities*, and of discovering automatically all possible relations of a certain kind (co-circularity, parallelism, perpendicularity, etc) among the elements of a construction involving a chosen element, or all elements of a construction.

Moreover, GeoGebra Discovery introduces a new feature: the possibility, through the *ShowProof* command [13], of displaying in the GeoGebra Discovery CAS window the different algebraic steps internally performed by the program to confirm or deny a given statement, as well as a *measure of the complexity* of the proved statement, defined (see [13] for details) as the maximum degree of the polynomials f_i , such that $t = f_1 h_1 + \dots + f_r h_r$, or such that $1 = f_1 h_1 + \dots + f_r h_r + f_{r+1} * (zt - 1)$, where t is the thesis and $h_1, \dots, h_r$ are the hypotheses.

Let us remark that all these features are accomplished through the internal performance of symbolic computation algorithms, which implies the formal validity of the obtained results. See [4], where, concerning the use of algebraic automated deduction methods, it is declared that

... This paper describes the formalization of the arithmetization of Euclidean plane geometry ... The arithmetization of geometry paves the way for the use of algebraic automated deduction methods in synthetic geometry. Indeed, without a “back-translation” from algebra to geometry, algebraic methods only prove theorems about polynomials and not geometric statements. However, thanks to the arithmetization of geometry, the proven statements correspond to theorems of any model of Tarski’s Euclidean geometry axioms. ...

2. CHATGPT AND GEOGEBRA DISCOVERY

Chatbots, such as ChatGPT [7], are popular Large Language Models that have been recently subject to different studies concerning the relation with mathematics (see the very recent paper [16], addressing mathematics olympiad problems with AlphaGeometry, a neural language model, or the more general references in [3]).

The goal of our contribution is to analyze and compare the behavior of these two kinds (ChatGPT/GeoGebra Discovery) of *artificial/automated* tools for dealing with mathematical issues. This comparison will be exhibited in three different contexts.

First, addressing, with GeoGebra Discovery, a problem of one of the fathers of Artificial Intelligence (A.I.), H. Gelernter, who presented, back in 1959, at a UNESCO meeting in Paris, a first *geometry-theorem proving machine*, [8]. And, one year later, described in this way its performance [9]:

In early spring, 1959, an IBM 704 computer, with the assistance of a program comprising some 20,000 individual instructions, proved its first theorem in elementary Euclidean plane geometry. Since that time, the geometry theorem-proving machine (a particular state configuration of the IBM 704 specified by the afore-mentioned machine code) has found solutions to a large number of problems taken from high school textbooks and final examinations in plane geometry ... the theorem-proving program relies upon heuristic methods to restrain it from generating proof sequences that do not

have a high a priori probability of leading to a proof for the theorem in question ... At this stage in its development, the geometry machine was capable of producing proofs that were quite impressive (Appendix I)... Three years ago, the dominant opinion was that the geometry machine would not exist today. And today, hardly an expert will contest the assertion that machines will be proving interesting theorems in number theory three years hence...

We have addressed with a laptop and GeoGebra Discovery the above mentioned problem from Appendix I in [9], showing that GeoGebra Discovery not only is able to check the correctness of the statement, but even to find by itself the thesis (the parallelism of certain two lines), as one of the many potential results holding on the given geometric construction. But we should also remark the optimistic perspective of Gelernter, when declaring, at the end of the above quote, the existence of geometry proving machines just three years after 1960!

Second, reporting the results of [3] dealing with ChatGPT/GeoGebra Discovery computation of geometric loci, concluding that

... Except in some simple cases, we showed that the chatbot is, at best, plausible, but not reliable. Either due to its making arithmetic errors, or by simply sketching a general guideline for solving the task, we cannot currently delegate ChatGPT for automating the search for loci. We also compared the ChatGPT results with those of GeoGebra, showing that the latter clearly surpasses the former for this particular task. However, we have also exhibited some cases showing that neither system is fully reliable.

Third, addressing with both GeoGebra Discovery and ChatGPT a non-trivial geometric inequality concerning the sides a, b, c of a triangle and the radius r of the incircle,

$$a^6 + b^6 + c^6 \geq 5148r^6$$

related to an AMS-Monthly Problem, see [15]. We will show how GeoGebra Discovery is capable of verifying the truth of such inequality instantaneously (but without yielding any information about the reasons for it), while ChatGPT produces a long list of arguments, relying on some other inequalities (without proof). Moreover, we used GeoGebra Discovery to check the correctness of ChatGPT intermediate statements.

We think –and argue in our contribution– that such cooperation protocol: using GeoGebra Discovery to verify the truth of ChatGPT, and using ChatGPT to exhibit arguments to support GeoGebra Discovery output, enhancing the best of both tools, could be of interest to analyze and to develop in a near future.

REFERENCES

- [1] M. Abánades, F. Botana, Z. Kovács, T. Recio, and C. Sólyom-Gecse, *Development of automatic reasoning tools in GeoGebra*, ACM Communications in Computer Algebra **50** (2016), no. 3, 85–88, DOI 10.1145/3015306.3015309
- [2] F. Botana, Z. Kovács, and T. Recio, *A mechanical geometer*, Mathematics in Computer Science **15** (2021) 631–641, DOI 10.1007/s11786-020-00497-7
- [3] F. Botana, and T. Recio, *Geometric Loci: Caveat Emptor!*, Computation, **12**(2), 30 (2024) <https://doi.org/10.3390/computation12020030>
- [4] P. Boutry, G. Braun, and J. Narboux, *Formalization of the arithmetization of Euclidean plane geometry and applications*, Journal of Symbolic Computation **90** (2019), 149–168, DOI 10.1016/j.jsc.2018.04.007

- [5] C. Brown, Z. Kovács, T. Recio, R. Vajda, and M.P. Vélez, *Is Computer Algebra Ready for Conjecturing and Proving Geometric Inequalities in the Classroom?* Mathematics in Computer Science **16** (2022), no. 31, DOI 10.1007/s11786-022-00532-9
- [6] C. Brown, Z. Kovács, T. Recio, R. Vajda, R., and M.P. Vélez, *GeoGebra Discovery*, In: C. Dubois, M. Kerber (eds), Intelligent Computer Mathematics, Proceedings of the 16th International Conference CICM, Lecture Notes in Computer Science, Springer 2023, DOI 10.1007/978-3-031-42753-4
- [7] ChatGPT: Optimizing Language Models for Dialogue. Available online: <https://openai.com/blog/chatgpt/>.
- [8] H. Gelernter, *Realization of a geometry-theorem proving machine*. English, with English French, German, Russian, and Spanish summaries. Information processing. Proceedings of the International Conference on Information Processing, Unesco, Paris 15–20 June 1959, Unesco Paris, R. Oldenbourg, Munich, and Butterworths, London, 1960, pp. 273–282.
- [9] H. Gelernter, J. Hansen, D. Loveland, *Empirical Explorations of the Geometry-Theorem Proving Machine*. Western Joint IRE-AIEE-ACM Computer Conference, San Francisco, California, 3–5 May 1960, 143–149. <https://doi.org/10.1145/1460361.1460381>
- [10] Z. Kovács, T. Recio, and M.P. Vélez, *Detecting truth, just on parts* Revista Matemática Complutense **32** (2019), 451–474, DOI 10.1007/s13163-018-0286-1
- [11] Z. Kovács, T. Recio, and M.P. Vélez, *Automated reasoning tools in GeoGebra Discovery*, ISSAC 2021 Software Presentations, ACM Communications in Computer Algebra **55** (2021), no. 2, Issue 216, 39–43, DOI 10.1145/3493492.3493495
- [12] Z. Kovács, T. Recio, and M.P. Vélez, *Automated reasoning tools with GeoGebra: What are they? What are they good for?*, In: P. R. Richard, M. P. Vélez, S. van Vaerenbergh (eds): *Mathematics Education in the Age of Artificial Intelligence: How Artificial Intelligence can serve mathematical human learning*. Series: Mathematics Education in the Digital Era, Springer, 2022, 23–44. DOI 10.1007/978-3-030-86909-0_2
- [13] Z. Kovács, T. Recio, and M.P. Vélez, *Showing proof, assessing difficulty with GeoGebra Discovery*. In: Quaresma, P. and Kovács, Z. (Eds.), Proceedings 14th International Conference on Automated Deduction in Geometry, Electronic Proceedings in Theoretical Computer Science 398, Open Publishing Association, 2023, 43–52, DOI 10.4204/EPTCS.398.8
- [14] T. Recio, and M.P. Vélez, *Automatic Discovery of Theorems in Elementary Geometry*. Journal of Automated Reasoning **23** (1999), 63–82, DOI 10.1023/A:1006135322108
- [15] D. Sitaru, *Problem 11984*. American Mathematical Monthly **124** (2017), no. 5, 466, <http://www.jstor.org/stable/10.4169/amer.math.monthly.124.5.465>
- [16] T.H. Trinh, Y. Wu, Q. V. Quoc V. Le, H. He, and T. Luong, *Solving olympiad geometry without human demonstrations*. Nature, **625**, 2024, 476–482. <http://dx.doi.org/10.1038/s41586-023-06747-5>

Universidad de Vigo, Pontevedra, Spain.

Email address: fbotana@uvigo.gal

Universidad Antonio de Nebrija, Madrid, Spain.

Email address: trecio@nebrija.es

Universidad Antonio de Nebrija, Madrid, Spain.

Email address: pvelez@nebrija.es

DETERMINANT OF THE DISTANCE MATRIX OF A TREE

EMMANUEL BRIAND, LUIS ESQUIVIAS, ÁLVARO GUTIÉRREZ, ADRIÁN LILLO,
MERCEDES ROSAS

ABSTRACT. In this work, we present a combinatorial proof of the Graham–Pollak formula for the determinant of the distance matrix of a tree, via sign-reversing involutions and the Lindström–Gessel–Viennot lemma. Our approach provides a cohesive and unified framework for the understanding of the existing generalizations and q -analogues of the Graham–Pollak formula, and facilitates the derivation of a natural simultaneous generalizations for them.

1. INTRODUCTION

Consider a tree T with vertices labeled from one to n , and edge set E . The *distance* between vertices i and j , denoted by $d(i, j)$, is defined as the number of edges along the unique path connecting them in T . The *distance matrix* of T , denoted by $M(T)$, is then defined as $(d(i, j))_{1 \leq i, j \leq n}$. In their influential 1971 paper [GP71], Graham and Pollak established that the determinant of the distance matrix of T obeys what is now known as the *Graham–Pollak formula*:

$$(1) \quad \det M(T) = (-1)^{n-1} (n-1) 2^{n-2}.$$

Observe that this formula implies that the determinant of the distance matrix of T is solely dependent on its number of vertices, and not on its tree structure.

Multiple techniques drawn from linear algebra, ranging from Gauss elimination to Charles Dodgson’s condensation formula, have been used to prove the Graham–Pollak formula [DY20, GP71, GL78, Til10, YY07, ZD16]. However, the elegance of the expression $(-1)^{n-1} (n-1) 2^{n-2}$ suggests the existence of a signed enumeration problem solved by $\det M(T)$. Pursuing this trail has led us to a novel combinatorial proof of the Graham–Pollak formula that relies on the existence of sign-reversing involutions, and on the celebrated *Lindström–Gessel–Viennot lemma*. These constructions constitute the core of our findings. This paper ends illustrating how our combinatorial proof not only serves as a unified framework for existing generalizations and q -analogues of the Graham–Pollak formula but also allows for the derivation of a novel extension to the formula.

2. SKETCH OF THE PROOF

Throughout the text, we fix a tree $T = ([n], E)$ with vertex set $[n]$ and edge set E , where $[n]$ denotes the set of integers between one and n .

Given a permutation σ in $\mathbb{S}_n$ and a map $f : [n] \rightarrow E$, we say that the ordered pair (σ, f) is a *catalyst for T* if for each vertex i , we have that edge $f(i)$ lies in the path $P(i, \sigma(i))$. A straightforward combinatorial argument reveals that

$$\det M(T) = \sum_{\sigma \in \mathbb{S}_n} \prod_{i=1}^n d(i, \sigma(i)) = \sum_{(\sigma, f) \in K} \text{sign}(\sigma).$$

where K represents the set of all catalyst for T .

For each catalyst $(\sigma, f) \in K$ we associate the directed multigraph with vertex set $[n]$ and edges multiset $\{\{\vec{f}(i) \mid i \in v\}\}$, where $\vec{f}(i)$ denotes the edge $f(i)$ oriented from i to $\sigma(i)$. That constitutes the *arrowflow* induced by (σ, f) . An arrowflow is deemed *unital* if the undirected graph it induces is connected and contains no repeated oriented edges. We say that it is *zero-sum* otherwise.

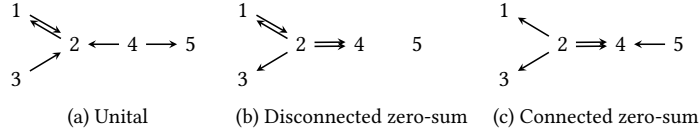


FIGURE 1. The different kinds of arrowflows.

Expanding on the concept of an arrowflow, we introduce the *arrowflow partition* of the set of catalysts for T , by asserting that two catalysts inducing the same arrowflow are equivalent. Those classes are also designated as either zero-sum or unital, as naturally inferred.

The Graham–Pollak formula becomes transparent when expressed in terms of the arrowflow partition. Our main theorem asserts that the signed sum of catalysts within a zero-sum class is always equal to zero, while in a unital class, it corresponds to $(-1)^{n-1}$. Now, a straightforward counting argument neatly concludes the derivation of the Graham–Pollak formula.

The theorem’s proof for zero-sum classes derives from an elegant sign-reversing involution with no fixed points. In contrast, the examination of unital ones requires more intricate arguments. Specifically, given a unital arrowflow A with arrowflow class $C(A)$, we construct a gigantic acyclic directed multigraph, termed the *route map* of A and denoted by $\mathcal{R}_A$. Subsequently, we illustrate how each catalyst in $C(A)$ induces a family of n paths on $\mathcal{R}_A$. Leveraging on the Lindström–Gessel–Viennot Lemma, we deduce that the signed sum of all catalysts in $C(A)$ corresponds to the signed count of non-intersecting n -paths on $\mathcal{R}_A$. The arguments concludes by establishing the existence of a unique non-intersecting family of n -paths originating from a catalyst in $C(A)$. Furthermore, we show that the underlying permutation is an n -cycle, giving the desired sign.

3. BEYOND THE GRAHAM-POLLAK FORMULA

Various generalizations of the Graham–Pollak formula exist in the literature. A version of the Graham–Pollak formula for simple trees with weighted edges is presented in [BKN05], while the situation of arc-weighted trees is treated in [BLP09]. In both cases, the weight of a path is defined as the sum of the weights of its edges. On the other hand, q -analogues of these results are also present in the literature. In them, the distance between vertices is defined using q -integers. Simple trees obey the q -Graham–Pollak formula [YY07, Cor. 2.3], $(-1)^{n-1}(n-1)(1-q)^{n-2}$. A q -analogue for trees weighted with integers appears in the same work, [YY07, Thm. 2.4]. There also exist q -analogues for the Graham–Pollak formula when T is arc-weighted with integers [BLP09, Thm. 3.1], or over a commutative ring [ZD16, Thm. 4], or with matrices over a commutative ring [ZD16, Thm. 7].

Our combinatorial proof of the Graham–Pollak formula not only provides a foundation for understanding existing generalizations as outlined above, but also paves the way for the creation of a new one. The novel idea is to define the distance between two vertices using the operation q -sum, that we denote by $\oplus$ and define as

$$a \oplus b = a + b + (q-1)ab.$$

Using the operation of q -sum, we simplify [YY07, Thm. 2.4], by noting that $[1]_q = 1$ and $[a + b]_q = [a]_q \oplus [b]_q$.

Let e^+ and e^- be the arcs originating from edge e , and let $E^\pm$ be the set of arcs of T where there is an arc pointing in each possible direction. Let R be a commutative ring, and $\alpha : E^\pm \rightarrow R[q]$ be a *weight function*. Define the q -distance between vertices i and j as

$$d_q(i, j) = \alpha(i_0, i_1) \oplus \alpha(i_1, i_2) \oplus \cdots \oplus \alpha(i_{k-1}, i_k).$$

where $i_0, i_1, \dots, i_k$ is the unique path from $i = i_0$ to $j = i_k$.

With this conditions, the determinant of the d_q -distance matrix of a tree T is

$$(2) \quad \det M(T) = (-1)^{n-1} \sum_{e \in E} \left(\alpha_e \alpha_{e^-} \prod_{\substack{f \in E \\ f \neq e}} (\alpha_f \oplus \alpha_{f^-}) \right),$$

where we write α_a for $\alpha(a)$.

A similar reasoning also provides a combinatorial proof for the Choudhury–Khare formula [CK19, Thm. A]. We highlight that, while that generalization is, in a precise sense, the most general possible [CK19, Example 1.13], Equation (2) stands independently. It represents the most natural simultaneous generalization of [ZD16, Thm. 4] and [YY07, Thm. 2.4].

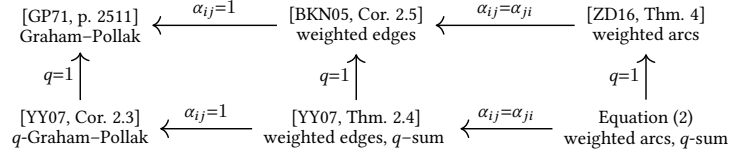


FIGURE 2. Relationship between the formulas found in the literature.

ACKNOWLEDGEMENTS

We dedicate this work to Ira Gessel as a token of our gratitude for his lecture on the Lindström–Gessel–Viennot lemma, which he virtually delivered at the University of Seville in march of 2022 [Ges22]. The senior authors would also like to express their gratitude to Xavier Viennot for the entrancing memories of his lectures.

This work has been partially supported by the Grant PID2020-117843GB-I00 funded by MICIU/AEI/ 10.13039/501100011033 and by P2001056 (Junta de Andalucía, FEDER, PAIDI2020).

REFERENCES

- [BKN05] Ravindra B. Bapat, Stephen J. Kirkland, and Michael Neumann. On distance matrices and laplacians. *Linear Algebra and its Applications*, 401:193–209, 2005. Special Issue in honor of Graciano de Oliveira.
- [BLP09] Ravindra B. Bapat, Arbind K. Lal, and Sukanta Pati. The distance matrix of a bidirected tree. *Electron. J. Linear Algebra*, 18:233–245, 2009.
- [CK19] Projesh Nath Choudhury and Apoorva Khare. Distance matrices of a tree: two more invariants, and in a unified framework. *arXiv e-prints*, 2019, math.CO/1903.11566.
- [DY20] Zhibin Du and Jean Yeh. Another simple proof of Graham and Pollak’s theorem. *Discrete Math.*, 343(10):111994, 3, 2020.
- [Ges22] Ira Gessel. Nonintersecting paths in enumerative combinatorics, 2022. Online talk at the seminar “Combinatoria Algebraica en Sevilla”.
- [GL78] Ronald L. Graham and László Lovász. Distance matrix polynomials of trees. In *Problèmes combinatoires et théorie des graphes (Colloq. Internat. CNRS, Univ. Orsay, Orsay, 1976)*, volume 260 of *Colloq. Internat. CNRS*, pages 189–190. CNRS, Paris, 1978.
- [GP71] Ronald L. Graham and Henry O. Pollak. On the addressing problem for loop switching. *Bell System Tech. J.*, 50:2495–2519, 1971.
- [Til10] Valerie Tillia. Determinants of distance matrices of trees. Master’s thesis, Portland State University, 2010.
- [YY07] Weigen Yan and Yeong-Nan Yeh. The determinants of q -distance matrices of trees and two quantiles relating to permutations. *Adv. in Appl. Math.*, 39(3):311–321, 2007.
- [ZD16] Hui Zhou and Qi Ding. The distance matrix of a tree with weights on its arcs. *Linear Algebra and its Applications*, 511:365–377, 2016.

CONSTRUCTION OF BIRATIONAL TRILINEAR VOLUMES VIA TENSOR RANK CRITERIA

LAURENT BUSÉ AND PABLO MAZÓN

ABSTRACT. We provide effective methods to construct and manipulate trilinear birational maps $\phi : (\mathbb{P}^1)^3 \dashrightarrow \mathbb{P}^3$ by establishing a novel connection between birationality and tensor rank. This is the first family of nonlinear birational transformations between 3D spaces that can be operated with enough flexibility for applications in computer-aided geometric design [8, §7]. More precisely, we describe the geometric constraints on the defining control points of the map that are necessary for birationality, and present constructions for such configurations. For adequately constrained control points, we prove that birationality is achieved if and only if a certain $2 \times 2 \times 2$ tensor has rank one. As a corollary, we prove that the locus of weights that ensure birationality is the Segre variety $\sigma(\mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1)$. Additionally, we provide formulas for the inverse ϕ^{-1} as well as the explicit defining equations of the irreducible components of the base loci. Finally, we introduce a notion of “distance to birationality” for trilinear rational maps, and explain how to continuously deform birational maps. This extended abstract is based on [6], which has been submitted for publication at a journal.

INTRODUCTION

In the fields of geometric modeling and computer-aided geometric design (CAGD), rational maps play a pivotal role. They offer an intuitive means of representing curves, surfaces, and volumes [5, 7, 3]. The primary representation of rational parametrizations in practical scenarios involve control points, nonnegative weights, and blending functions. For rational volumes, the typical parametrizations take the form

$$(1) \quad \phi : \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1 \dashrightarrow \mathbb{P}^3$$

$$(s_0 : s_1) \times (t_0 : t_1) \times (u_0 : u_1) \mapsto \sum_{i=0}^n \sum_{j=0}^m \sum_{k=0}^l w_{ijk} \mathbf{P}_{ijk} b_i^n(s_0, s_1) b_j^m(t_0, t_1) b_k^l(u_0, u_1),$$

for some *control points* $\mathbf{P}_{ijk} = (1, x_{ijk}, y_{ijk}, z_{ijk})$ in $\mathbb{R}^4$ and nonnegative *weights* w_{ijk} in $\mathbb{R}$, for each $0 \leq i \leq n, 0 \leq j \leq m, 0 \leq k \leq l$, where $b_l^N(x_0, x_1)$ is the l -th homogeneous Bernstein polynomial of degree N .

A rational parametrization is *birational* if it admits an inverse map which is also rational. Birational maps have several advantages in applications, since the inverse can be exploited for computing preimages. Some applications require the computation of preimages for

The two authors have received funding from the European Union’s “Horizon 2020 research and innovation programme”, under the Marie Skłodowska-Curie grant agreement n° 860843.

The talk at the meeting EACA 2024 is proposed by the second author.

various purposes, and it is convenient for others such as image and volume warping, morphing, texturing, or the generation of 3D curved meshes for geometric analysis.

In general, (1) is not birational. More specifically, the locus of birational transformations in the space of such parametrizations generally has a large codimension (see e.g. [1, 2, 4]). Therefore, birationality represents a notably restrictive condition, making the construction of birational maps a challenging algebraic problem that should be treated using tools from algebraic geometry and commutative algebra.

1. PREVIOUS WORK

Surprisingly, although birational geometry is a classical topic in algebraic geometry with a trajectory of over 150 years, it wasn't until 2015 that the practical application of (nonlinear) birational transformations to design emerged, in the work of Thomas Sederberg and collaborators [9, 8]. The earliest works about constructing birational maps dealt with 2D tensor-product parametrizations $\phi : \mathbb{P}_{\mathbb{R}}^1 \times \mathbb{P}_{\mathbb{R}}^1 \dashrightarrow \mathbb{P}_{\mathbb{R}}^2$ defined by polynomials of low degree. Recently, novel conditions for birationality have been proposed for parametrizations $\phi : \mathbb{P}_{\mathbb{R}}^2 \dashrightarrow \mathbb{P}_{\mathbb{R}}^2$ with quadratic entries, relying on the complex rational representation of a rational map [11, 10].

2. CONSTRUCTION OF TRILINEAR BIRATIONAL MAPS

In this work, we are interested in trilinear birational maps.

Definition 2.1. A trilinear rational map is a rational map $\phi : (\mathbb{P}^1)^3 \dashrightarrow \mathbb{P}^3$ defined by trilinear polynomials. Using control points and weights, it can be defined as

$$(2) \quad \phi : \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1 \dashrightarrow \mathbb{P}^3$$

$$(s_0 : s_1) \times (t_0 : t_1) \times (u_0 : u_1) \mapsto (f_0 : f_1 : f_2 : f_3) = \sum_{0 \leq i,j,k \leq 1} w_{ijk} \mathbf{P}_{ijk} b_i^1(s_0, s_1) b_j^1(t_0, t_1) b_k^1(u_0, u_1).$$

If ϕ is birational, the inverse ϕ^{-1} has the form

$$(3) \quad \phi^{-1} : \mathbb{P}^3 \dashrightarrow \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$$

$$(x_0 : x_1 : x_2 : x_3) \mapsto (A_0 : A_1) \times (B_0 : B_1) \times (C_0 : C_1),$$

where $A_i = A_i(x_0, x_1, x_2, x_3)$ (resp. $B_j = B_j(x_0, x_1, x_2, x_3)$ and $C_k = C_k(x_0, x_1, x_2, x_3)$) are homogeneous of the same degree for $i = 0, 1$ (resp. $j = 0, 1$ and $k = 0, 1$), without a common factor.

Definition 2.2. If ϕ is birational, the type of ϕ is the triple $(\deg A_i, \deg B_j, \deg C_k)$ in $\mathbb{Z}^3$.

Birationality imposes geometric constraints on the control points, that are formalized in the following four classes of trilinear rational maps: *hexahedral*, *pyramidal*, *scaffold*, and *tripod*. Each of these classes are depicted in FIGURE 1, and respectively correspond to birational maps of type $(1, 1, 1)$, $(1, 1, 2)$, $(1, 2, 2)$, and $(2, 2, 2)$. Specifically, we have the following definitions.

Definition 2.3. The boundary surfaces Σ_i, T_j, Y_k are the closure of the images by ϕ of

$$(s_0 : s_1) = (1 : i), (t_0 : t_1) = (1 : j), (u_0 : u_1) = (1 : k),$$

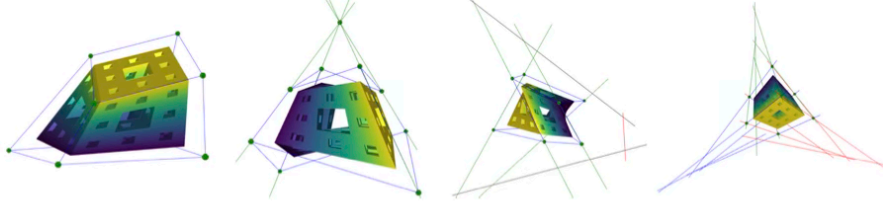


FIGURE 1. The distinct geometric constraints on the control points that are necessary for birationality.

for each $0 \leq i, j, k \leq 1$. For the same indices, the boundary s -, t -, and u -lines are respectively defined as

$$s_{jk} = \overline{\mathbf{P}_{0jk}\mathbf{P}_{1jk}}, \quad t_{ik} = \overline{\mathbf{P}_{i0k}\mathbf{P}_{i1k}}, \quad u_{ij} = \overline{\mathbf{P}_{ij0}\mathbf{P}_{ij1}}.$$

Definition 2.4. Let all the boundary surfaces be smooth and pairwise distinct.

- (1) ϕ is hexahedral if all the boundary surfaces are planes
- (2) ϕ is pyramidal if all the boundary lines in one parameter meet at a point, and the boundary surfaces in the same parameter are quadrics
- (3) ϕ is scaffold if the boundary surfaces in one parameter are planes that intersect at a line ℓ , the boundary surfaces in the other two parameters are quadrics, and there are two lines that intersect ℓ and all the parametric lines in the first parameter
- (4) ϕ is tripod if all the boundary surfaces are quadrics, the four boundary s -lines (resp. t - and u -) intersect a line s (resp. t and u), the lines s, t, u intersect at a common point, and all the boundary lines intersect a plane conic that meets s, t, u .

The following theorem establishes that birationality boils down to a rank-one condition on a $2 \times 2 \times 2$ tensor. It relates birationality, the existence of specific syzygies between the defining polynomials of ϕ , and tensor rank. Moreover, it is effective for constructive results.

Theorem 2.5. Let ϕ be either hexahedral, pyramidal, scaffold, or tripod. Then, ϕ is birational of the corresponding type if and only if the $2 \times 2 \times 2$ tensor

$$(4) \quad W = \left(\frac{w_{ijk}}{\Delta_{ijk}} \right)_{0 \leq i, j, k \leq 1}$$

has rank one, where Δ_{ijk} are rational functions in the coordinates of the control points.

The most relevant computational advantage of birational maps is the efficient and exact computation of preimages. The following result presents explicit formulas for the inverse of a hexahedral birational map. Moreover, it describes the contractions and blow-ups of the birational map.

Theorem 2.6. Let ϕ be either hexahedral, pyramidal, scaffold, or tripod. If the rank-one condition of Theorem 2.5 holds, then ϕ^{-1} is given by

$$(5) \quad (x_0 : x_1 : x_2 : x_3) \mapsto (\alpha_1 \sigma_1 : \alpha_0 \sigma_0) \times (\beta_1 \tau_1 : \beta_0 \tau_0) \times (\gamma_1 v_1 : \gamma_0 v_0),$$

where σ_i, τ_j, v_k are the defining polynomials of the boundary surfaces of ϕ , and $\alpha_i, \beta_j, \gamma_k$ relate to the factorization of the tensor W . Additionally:

- (1) We provide explicitly a minimal set of generators for the base ideal $I = (f_0, f_1, f_2, f_3)$
- (2) We describe the blow-ups and blow-downs of ϕ

REFERENCES

- [1] Cinzia Bisi, Alberto Calabri, and Massimiliano Mella. “On plane Cremona transformations of fixed degree”. In: *J. Geom. Anal.* 25.2 (2015), pp. 1108–1131. ISSN: 1050-6926. DOI: [10.1007/s12220-013-9459-9](https://doi.org/10.1007/s12220-013-9459-9). URL: <https://doi.org/10.1007/s12220-013-9459-9>.
- [2] Dominique Cerveau and Julie Déserti. *Transformations birationnelles de petit degré*. Vol. 19. Cours Spécialisés [Specialized Courses]. Société Mathématique de France, Paris, 2013, pp. viii+223. ISBN: 978-2-85629-770-4.
- [3] David A. Cox. *Applications of polynomial systems*. Vol. 134. CBMS Regional Conference Series in Mathematics. With contributions by Carlos D’Andrea, Alicia Dickenstein, Jonathan Hauenstein, Hal Schenck and Jessica Sidman. American Mathematical Society, Providence, RI, [2020] ©2020, pp. ix+250. ISBN: 978-1-4704-5137-0.
- [4] Julie Déserti and Frédéric Han. “On cubic birational maps of $\mathbb{P}_{\mathbb{C}}^3$ ”. In: *Bull. Soc. Math. France* 144.2 (2016), pp. 217–249. ISSN: 0037-9484. DOI: [10.24033/bsmf.2712](https://doi.org/10.24033/bsmf.2712). URL: <https://doi.org/10.24033/bsmf.2712>.
- [5] Gerald Farin. *Curves and surfaces for computer-aided geometric design: a practical guide*. Elsevier, 2014.
- [6] Pablo González-Mazón and Laurent Busé. *Construction of birational trilinear volumes via tensor rank criteria*. 2023.
- [7] Les Piegl and Wayne Tiller. *The NURBS book*. Springer Science & Business Media, 1996.
- [8] Thomas W. Sederberg, Ronald N. Goldman, and Xuhui Wang. “Birational 2D free-form deformation of degree $1 \times n$ ”. In: *Comput. Aided Geom. Design* 44 (2016), pp. 1–9. ISSN: 0167-8396. DOI: [10.1016/j.cagd.2016.02.020](https://doi.org/10.1016/j.cagd.2016.02.020). URL: <https://doi.org/10.1016/j.cagd.2016.02.020>.
- [9] Thomas W. Sederberg and Jianmin Zheng. “Birational quadrilateral maps”. In: *Comput. Aided Geom. Design* 32 (2015), pp. 1–4. ISSN: 0167-8396. DOI: [10.1016/j.cagd.2014.11.001](https://doi.org/10.1016/j.cagd.2014.11.001). URL: <https://doi.org/10.1016/j.cagd.2014.11.001>.
- [10] Xuhui Wang et al. “Birational Quadratic Planar Maps with Generalized Complex Rational Representations”. In: *Mathematics* 11.16 (2023), p. 3609.
- [11] Xuhui Wang et al. “Constructing quadratic birational maps via their complex rational representation”. In: *Comput. Aided Geom. Design* 85 (2021), Paper No. 101969, 11. ISSN: 0167-8396, 1879-2332. DOI: [10.1016/j.cagd.2021.101969](https://doi.org/10.1016/j.cagd.2021.101969). URL: <https://doi.org/10.1016/j.cagd.2021.101969>.

Université Côte d’Azur, Inria, 2004 route des Lucioles, 06902 Sophia Antipolis, France.
Email address: laurent.buse@inria.fr

Università di Trento, Dipartimento di Matematica, Via Sommarive 14, 38123 Povo, Trento, Italy.
Email address: pablo.gonzalezmazon@unitn.it

ALGEBRAIC METHODS IN CELL DIFFERENTIATION

ELENA CAMACHO AGUILAR, FRANCISCO CASTRO JIMÉNEZ,
AND FRANCISCO GARCÍA CORTÉS

ABSTRACT. We apply Groebner cover techniques to a system of polynomial equations with parameters inspired by the popular French Flag model for patterning in Biology. We interpret the obtained solutions of the system as the possible states of a certain cell, which is defined by the expression of a set of proteins.

INTRODUCTION

Understanding how complex networks of genes or proteins interpret information to produce organs with specific sizes, shapes, and patterns to generate an adult organism has been the focus of many years of research, yet it is still far from being completely understood. New mathematical approaches are needed to simplify the study of the mechanisms that govern these biological processes.

The problem discussed here is inspired by the *French Flag model* (FFm), a classical framework for explaining how a single inductive signal can drive the differentiation of cells and the patterning of a tissue during embryonic development [6]. In FFm, the diffusion of a signal (referred to as *morphogen*) from a source cell creates a spatial signaling gradient which is translated into a pattern by the nearby cells interpreting the level of morphogen concentration they are exposed to (Fig. 1). In particular, cells that are exposed to a low morphogen concentration, remain in their initial state (red in Fig. 1A). Under middle concentrations of the morphogen, cells differentiate to cell type 2 (white in Fig. 1A). While under high concentrations, cells differentiate to cell type 3 (blue in Fig. 1A).

Here we focus on a system inspired by the FFm. We consider three simple mathematical equations that describe how a single morphogen signal β can control the expression of three genes S, B, C in a cell, defining the state of such cell (Fig. 1B) [1, App., p. 299]. Stable states in this system correspond to cell types that the cell can differentiate to. Our goal is to understand the characteristics of this model, for example, the space of solutions to the system and how it depends on its parameters.

1. THREE GENES AND ONE MORPHOGEN

Following [1, App. p. 299], we are going to deal with a model for how a single morphogen could control cell differentiation into three cell types. In this model it is assumed that gene expression in time is controlled by the following dynamical system (1). We have changed

The first author has been partially supported by the María de Maeztu strategic plan (CEX2020-001088-M) awarded to the Centro Andaluz de Biología del Desarrollo (CABD).

Second and third authors are partially supported by PID2020-117843GB-I00.

The talk at the meeting EACA 2024 has been given by the second author.

2 ELENA CAMACHO AGUILAR, FRANCISCO CASTRO JIMÉNEZ, AND FRANCISCO GARCÍA CORTÉS

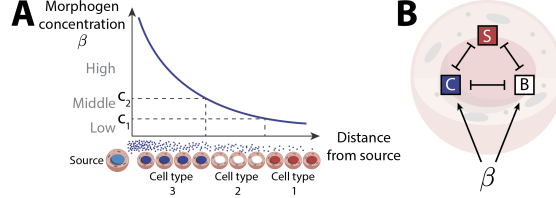


FIGURE 1. French Flag model, FFm. (A) The three cell types (blue, white and red) are determined through the three different morphogen concentrations (high, middle, low), defined by two thresholds c_1 y c_2 . (B) Network proposed to model process described in (A).

the names of the variables and parameter from the original cited paper. New variables are B, C, S , corresponding to the gene expression levels, and the signaling parameter is β , that corresponds to the concentration of the morphogen.

$$\begin{aligned}
 \frac{dC}{dt} &= a_1 \frac{(\beta/k_{\beta 1})^{n_{\beta 1}}}{(1 + (\beta/k_{\beta 1})^{n_{\beta 1}})(1 + (B/k_{21})^{n_{21}} + (S/k_{31})^{n_{31}})} - \delta_1 C \\
 \frac{dB}{dt} &= a_2 \frac{(\beta/k_{\beta 2})^{n_{\beta 2}}}{(1 + (\beta/k_{\beta 2})^{n_{\beta 2}})(1 + (C/k_{12})^{n_{12}} + (S/k_{32})^{n_{32}})} - \delta_2 B \\
 \frac{dS}{dt} &= a_3 \frac{1}{1 + (C/k_{13})^{n_{13}} + (B/k_{23})^{n_{23}}} - \delta_3 S.
 \end{aligned}
 \tag{1}$$

The parameters n_{ij}, k_{ij} , with $i \in \{\beta, 1, 2, 3\}$, $j \in \{1, 2, 3\}$, are the *Hill coefficients* and *dissociation constants* respectively, and a_i, δ_i with $i \in \{1, 2, 3\}$ are the *production* and *degradation rates*, respectively (see [1, p. 299] for a biological interpretation of these parameters).

In [1], the system of differential equations (1) is simulated with initial condition $B = C = 0$ and $S = 2$, and with specific values for all the parameters except β [1, Table A1].

In the present work we only fix the values for the parameters n_{ij} , that appear as exponents in the expression of (1), and consider the remaining parameters as free parameters.

The original paper [1] aimed to find a simple model that could reproduce the behavior described by the FFm. Therefore, the values of the Hill coefficients n_{ij} were chosen as low as possible as long as the parameter β could control the presence of three different steady states, characterized by either S, B , or C high and the rest of variables low. In particular, $n_{ij} = 1$ with $i \in \{\beta, 1, 2, 3\}$, $j \in \{1, 2, 3\}$, except $n_{\beta 2} = 5$, fulfilled these requirements.

We are interested in (the structure of) the equilibrium points $\mathcal{E}$ of this new system, depending on the parameters (i.e. the set of points $(B(t), C(t), S(t))$ such that $dB(t)/dt = dC(t)/dt = dS(t)/dt = 0$). The polynomial system defining the algebraic set $\mathcal{E}$ is the following:

$$\begin{aligned}
 f_1 &= C(1 + k_{21}B + k_{31}S) - V_1 = 0 \\
 f_2 &= B(1 + k_{12}C + k_{32}S) - V_2 = 0 \\
 f_3 &= S(1 + k_{13}C + k_{23}B) - V_3 = 0.
 \end{aligned}
 \tag{2}$$

We have simplified notations by writing k_{ij} instead of $1/k_{ij}$, $V_3 = \frac{a_3}{\delta_3}$, and $V_k = \frac{b_k}{c_k}$ where $b_k = a_k \left(\frac{\beta}{k_{\beta k}}\right)^{n_{\beta k}}$ and $c_k = \delta_k \left(1 + \left(\frac{\beta}{k_{\beta k}}\right)^{n_{\beta k}}\right)$ for $k = 1, 2$, where we recall that $n_{\beta 1} = 1$ and $n_{\beta 2} = 5$, [1, p. 255]. So, in the previous system, the space of new parameters $\mathcal{P}(=\mathbb{C}^9)$ has coordinates $(\mathbf{k}, \mathbf{V}) := (k_{ij}, V_k)$. At the generic point $(\mathbf{k}, \mathbf{V})$ in $\mathcal{P}$, the equilibrium point set $\mathcal{E}$ is the intersection of three quadrics in the affine three dimensional space on the field $\mathbb{C}(\mathbf{k}, \mathbf{V})$. So, we can use Groebner basis techniques to describe $\mathcal{E}$ for generic points $(\mathbf{k}, \mathbf{V})$.

The reduced Groebner basis **GB** (w.r.t. the lexicographical ordering with $B > C > S$) of the ideal – in $\mathbb{Q}(\mathbf{k}, \mathbf{V})[B, C, S]$ – generated by $\{f_1, f_2, f_3\}$, has three polynomials of the form (known as *Shape Lemma form*; see e.g. [3], [2]):

$$(3) \quad F(S), B + F_1(S), C + F_2(S)$$

where $F(S), F_1(S), F_2(S)$ are univariate polynomials in S (which we omit here due to their length), of degree 5, 4, 4 respectively, with coefficients in the field $\mathbb{Q}(\mathbf{k}, \mathbf{V})$.

This generic **GB** gives a first insight on the solutions of the system. We are also interested in *special points* (i.e. *non-generic points*, which are also important from a biological point of view).

We apply *Groebner cover* techniques (see [4, Ch. 5]; see also [5]) to describe the shape of the solution space as a function of the parameters. Although this is still a work in progress, we show that, despite the simplicity of the system (2), the structure of the parametric solution set is more complex than expected. In a future work we will give biological meaning to the points in each stratum in the Groebner cover **GC**.

2. THE GROEBNER COVER **GC**

Instead of applying the command **grobcov** (in the *Singular* library **grobcov.lib**), we leverage the Buchberger's algorithm step-by-step on our system of original parametric polynomials in (2) with coefficients in the polynomial ring $\mathbb{Q}[\mathbf{k}, \mathbf{V}]$.

In order to simplify notations, let us define the following auxiliary polynomials:

$$\begin{aligned} \mathbf{det} &:= k_{12}k_{23}k_{31} + k_{13}k_{32}k_{21}, \\ \ell_1 &:= \mathbf{det} \cdot (k_{12}k_{23}V_1 - k_{23}k_{21}V_2 + k_{32}k_{21}V_3) + k_{21}k_{12}k_{23}(k_{32} - k_{31}), \\ \ell_2 &:= \mathbf{det} \cdot (k_{12}(k_{13}k_{21} + k_{12}k_{23})V_1 - k_{21}(k_{13}k_{21} + k_{12}k_{23})V_2 + k_{21}k_{12}(k_{32} - k_{31})V_3 \\ &\quad + k_{21}k_{12}(k_{32} - k_{31})(k_{12}k_{23} + k_{21}k_{13})). \end{aligned}$$

For $f \in \mathbb{C}[\mathbf{k}, \mathbf{V}]$, we denote $\mathcal{V}(f)$ the vanishing set of f in $\mathcal{P}$ and $D(f) = \mathcal{P} \setminus \mathcal{V}(f)$.

We are mainly interested in the *biologically driven* Groebner cover **bdGC**, i.e., the one that makes sense biologically instead of the *abstract GC*. We slightly simplify strata in the **GC** by assuming that the parameters can take only real values and that $k_{ij} > 0$, and so $\mathbf{det} > 0$. Moreover, $a_3 > 0$ (a_3 is the production rate of a protein) and then $V_3 = a_3/\delta_3 \neq 0$.

The simplified strata in **bdGC** are:

$$(4) \quad \Sigma_0 := D(\mathbf{det} k_{21} k_{23} \ell_1 \ell_2 V_3) = D(\ell_1 \ell_2), \quad \Sigma_{11} := \mathcal{V}(\ell_1), \quad \Sigma_{12} := D(\ell_1) \cap \mathcal{V}(\ell_2).$$

The stratum $\mathcal{V}(\ell_1, \ell_2)$ does not appear in **bdGC** since the variety $\mathcal{V}(\ell_1, \ell_2)$ is included in $\mathcal{V}(V_3)$ and we assume $V_3 \neq 0$.

In the open stratum Σ_0 the Groebner basis **GB**₀ is precisely the *generic* one **GB** (3).

4 ELENA CAMACHO AGUILAR, FRANCISCO CASTRO JIMÉNEZ, AND FRANCISCO GARCÍA CORTÉS

In the closed stratum Σ_{11} the corresponding Groebner basis $\mathbf{GB}_{11}$ has similar shape to $\mathbf{GB}_0$, although the degree of the polynomials $F(S), F_1(S), F_2(S)$ are in this case 5, 4, 3 respectively.

In the locally closed stratum Σ_{12} the corresponding Groebner basis $\mathbf{GB}_{12}$ has four polynomials of the form

$$(5) \quad (aS + b)H(S), \quad B + J_1(S), \quad (aS + b)C + J_2(S), \quad d_2C^2 + d_1C + J_3(S),$$

where first $a = \ell_1$, $b = k_{21} \cdot \mathbf{det} \cdot V_3$, $d_2 = k_{23}k_{21}\ell_1$, and $d_1 = d_1(\mathbf{k}, \mathbf{V})$ is a certain polynomial, quadratic in $\mathbf{V}$. Moreover, H, J_1, J_2, J_3 are univariate in S of degree 3.

3. CONCLUSIONS

Here we show preliminary results to describe how the solutions to this biologically-inspired system depend on the parameters. Further work needs to be done to explore the biological meaning of these solutions. Despite considering a relatively simple system as a proof of concept, the methods described here can also be applied to more complex biological processes. For example, these processes could involve more genes and signals, which would be translated mathematically into systems of polynomial equations with higher dimensions and more parameters. Moreover, the degree of such polynomial equations could increase if we considered $n_{ij} \geq 2$.

In addition, we believe it would be interesting to leverage this approach for comparing different mathematical models for a common biological process through the structure of their solutions.

The authors offer their sincere thanks to the referee for his/her valuable comments.

REFERENCES

- [1] Camacho-Aguilar, E. and Warmflash, A. *Insights into mammalian morphogen dynamics from embryonic stem cell systems*. Current topics in developmental biology, 279–305, 137, (2020). <https://doi.org/10.1016/bs.ctdb.2019.11.010>.
<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7713707/>.
- [2] Cox, D. A. and D’Andrea, C. *Subresultants and the shape lemma*. Math. Comp. 92 (2023), no. 343, 2355–2379.
- [3] Giusti, M. Lecerf, G. and Salvy, B. *A Gröbner free alternative for polynomial system solving*. J. Complexity 17 (2001), no. 1, 154–211.
- [4] Montes, A. *The Gröbner Cover*. Algorithms and Computation in Mathematics, 27. Springer (2018).
- [5] Montes, A. and Wibmer, M. *Gröbner bases for polynomial systems with parameters*. J. Symbolic Comput., 45, (2010), 1391–1425, <https://doi.org/10.1016/j.jsc.2010.06.017>.
- [6] Wolpert, L. *Positional information and the spatial pattern of cellular differentiation*. Journal of theoretical biology, 1, 1–47. Vol. 25, (1969).

Andalusian Center for Developmental Biology (CABD)

Email address: ecamagu@upo.es

University of Seville

Email address: castro@us.es, fragarcor3@alum.us.es

SPARSE NULLSTELLENSATZ, RESULTANTS AND DETERMINANTS OF COMPLEXES

CARLOS D'ANDREA AND GABRIELA JERONIMO

ABSTRACT. We refine known results on the supports of a Bézout identity satisfied by a finite sequence of sparse Laurent polynomials without common zeroes in the toric variety associated to their supports. When the number of these polynomials is one more than the dimension of the ambient space, we obtain a formula for computing the sparse resultant as the determinant of a Koszul type complex.

Given a field K , and a finite sequence $f_1, \dots, f_k$ in $R_K := K[t_1, \dots, t_n]$, the classical *effective Hilbert's Nullstellensatz* deals with the problem of giving an effective procedure to decide if there is, and if so to compute, a *Bézout identity*

$$(1) \quad \sum_{i=1}^k g_i f_i = 1.$$

If degree bounds for the g_i 's are provided, then (1) turns into a computable Linear Algebra problem.

A first attempt to dealing with this problem can be done by homogenizing the input, i.e. considering $F_1, \dots, F_k \in \tilde{R}_K := K[t_0, \dots, t_n]$ which are the homogenizations of $f_1, \dots, f_k$ up to their total degrees $d_1, \dots, d_k$ respectively. We can then study the Koszul complex associated to this sequence:

$$(2) \quad \text{Kos}(\tilde{R}_K, F_1, \dots, F_k) : 0 \rightarrow \tilde{R}_K^{(k)} \xrightarrow{\Psi_k} \tilde{R}_K^{(k-1)} \xrightarrow{\Psi_{k-1}} \dots \xrightarrow{\Psi_2} \tilde{R}_K^{(1)} \xrightarrow{\Psi_1} \tilde{R}_K^{(0)} \rightarrow 0.$$

As this sequence is homogeneous, the maps in (2) are also graded as well, and hence we can consider the different graded pieces of it. For $d \in \mathbb{Z}_{\geq 0}$, the d -th graded part of $\text{Kos}(\tilde{R}_K, F_1, \dots, F_k)$ will be denoted by $\text{Kos}(\tilde{R}_K, F_1, \dots, F_k)_d$. The following result is well-known.

Theorem 1. *For $d \geq d_1 + \dots + d_k - n$, $\text{Kos}(\tilde{R}_K, F_1, \dots, F_k)_d$ is exact as a complex of K -vector spaces if and only if there are no common zeroes of $F_1, \dots, F_k$ in projective space $\mathbb{P}_{\tilde{K}}^n$.*

Theorem 1 produces a very sharp bound on the degrees of the g_i 's to produce a Bézout identity as in (1) at the cost of requiring the input not to have zeroes not only in affine

The first author has been partially supported by the Spanish MICINN research project PID2019-104047GB-I00, 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.

The second author has been partially supported by the Argentinian grants UBACYT 20020190100116BA and PIP 11220130100527CO CONICET.

The talk at the meeting EACA 2024 has been given by the first author.

space but in a compactification of it, the n -th dimensional projective space $\mathbb{P}_{\overline{K}}^n$. Indeed from the exactness of $Kos(\tilde{R}_K, F_1, \dots, F_k)_d$ one can find homogeneous $G_1, \dots, G_k$ such that $\sum_i G_i F_i = t_0^d$. By setting $t_0 = 1$, we recover $g_1, \dots, g_k$ such that $\deg(g_i) \leq d_1 + \dots + d_k - n - d_i$, satisfying (1), and hence solving the effective Nullstellensatz problem.

Of special interest is the so-called “codimension one” case, i.e. when $k = n + 1$. Here, tools from Elimination Theory like resultants can be used to deal with this problem. To introduce them, consider the following generic homogeneous polynomials in $n + 1$ variables $t_0, \dots, t_n$ of respective positive degrees $d_1, \dots, d_{n+1}$:

$$(3) \quad F_i^g := \sum_{\alpha \in \mathbb{Z}_{\geq 0}^{n+1}, |\alpha|=d_i} c_{i,\alpha} t^\alpha, \quad i = 1, \dots, n+1,$$

with each of the $c_{i,\alpha}$ being a new indeterminate. Set $\mathbb{K} := \mathbb{Q}(c_{i,\alpha})$. Note that the polynomials $F_1^g, \dots, F_{n+1}^g$ do not have common zeros in $\mathbb{P}_{\overline{\mathbb{K}}}^n$. Hence, the complex $Kos(\tilde{R}_{\mathbb{K}}, F_1^g, \dots, F_{n+1}^g)_d$ is exact for $d \geq d_1 + \dots + d_{n+1} - n$ thanks to Theorem 1. In the special case $n = 1$, $d = d_1 + d_2 - 1$, (2) reduces to only one nontrivial map between $\mathbb{K}$ -vector spaces of the same dimension $d_1 + d_2$, whose determinant equals the classical Sylvester resultant of the homogeneous bivariate forms F_1 and F_2 , see [CLO05, Chapter 3 §1]. This resultant can be generalized for $n > 1$: given positive degrees $d_1, \dots, d_{n+1}$, there is an irreducible polynomial $\text{Res}_{d_1, \dots, d_{n+1}} \in \mathbb{Z}[c_{i,\alpha}]$ called the resultant of $F_1^g, \dots, F_{n+1}^g$, which vanishes after a specialization of the $c_{i,\alpha}$ in a field K if and only if the specialized system arising from (3) after this specialization has a solution in the projective space over $\overline{K}$, see [CLO05, Chapter 3 §2] for its proper definition and basic properties.

In another direction, the determinant of a linear map among spaces of the same dimension with fixed bases can be generalized to the determinant of a finite exact complex of K -vector spaces of finite dimension, if one fixes bases in each of the non-zero terms of it. In practice, it involves the computation of maximal minors of all the nontrivial matrices representing the differentials in the aforementioned bases. This concept goes also all the way back to Cayley, see for instance [GKZ94, Appendix A]. Computational aspects can be found in [Dem84, Cha93].

The following is a classical result which generalizes the computation of the Sylvester resultant of two univariate polynomials by computing the determinant of a matrix.

Theorem 2. *For $d \geq d_1 + \dots + d_{n+1} - n$, we have that:*

- (1) *The determinant of the complex $Kos(\tilde{R}_{\mathbb{K}}, F_1^g, \dots, F_{n+1}^g)_d$ is equal to $\pm \text{Res}_{d_1, \dots, d_{n+1}}$.*
- (2) *This determinant can be computed as the gcd of the maximal minors of $\Psi_{1,d}$, the last nontrivial map in $Kos(\tilde{R}_{\mathbb{K}}, F_1^g, \dots, F_{n+1}^g)_d$.*
- (3) *Let K be any field. For homogeneous polynomials $F_1, \dots, F_{n+1} \in K[t_0, \dots, t_n]$ of respective degrees $d_1, \dots, d_{n+1}$, $Kos(\tilde{R}_K, F_1, \dots, F_{n+1})_d$ is exact if and only if $\text{Res}_{d_1, \dots, d_{n+1}}(F_1, \dots, F_{n+1}) \neq 0$.*

We present extensions of Theorems 1 and 2 to the sparse setting; proofs and details will appear in a forthcoming paper which is in preparation. To do this, we start with finite sets $\mathcal{A}_1, \dots, \mathcal{A}_k \subset \mathbb{Z}^n$. We will be working with a field K of characteristic zero, as our results are based on standard techniques in toric geometry which are defined over the complex

numbers. For $i = 1, \dots, k$, consider polynomials

$$(4) \quad f_i := \sum_{a \in \mathcal{A}_i} f_{i,a} t^a \in K[t_1^{\pm 1}, \dots, t_n^{\pm 1}],$$

with $f_{i,a} \in K^* := K \setminus \{0\}$. For short we denote with $K[t^{\pm 1}]$ the ring of Laurent polynomials $K[t_1^{\pm 1}, \dots, t_n^{\pm 1}]$. The torus $(K^*)^n$ will be denoted with $\mathbb{T}_K^n$. It is the natural environment to look for common zeroes of (4).

Set $P_i := \text{conv}(\mathcal{A}_i) \subset \mathbb{R}^n$ for the convex hull of $\mathcal{A}_i$, $i = 1, \dots, k$, and

$$P := P_1 + \dots + P_k.$$

If P is n -dimensional, there exists a *toric variety* X_P containing $\mathbb{T}_K^n$ and a polynomial ring S having as many variables as facets of P such that $f_1, \dots, f_k$ get “homogenized” to $F_1, \dots, F_k \in S$. Homogeneous here means with respect to the grading given by the Chow group of X_P . The feature of this homogenization is that $\xi \in \mathbb{T}_K^n$ is a common zero of the f_i ’s if and only if it is a common zero of the F_i ’s.

To deal with a more general problem, assume we are given another integral polytope $Q \subset \mathbb{R}^n$. Associated to the Minkowski sum $P + Q$ there is a toric variety X_{P+Q} “lying over” X_P , with its corresponding homogeneous coordinate ring S' and hence $f_1, \dots, f_k$ can also be homogenized to $F'_1, \dots, F'_k \in S'$.

For each of the facets of $P + Q$ there is an invariant Weil divisor associated to it. We will denote by $D_1, \dots, D_{n+r}$ these divisors. For a vertex v of $P + Q$ let α_v be the degree of $-\sum D_j$, the sum being over the divisors associated to all the facets containing v . Each of the F_i ’s has a degree α_{P_i} associated to its Newton polytope. Set $\alpha_P = \sum_{i=1}^k \alpha_{P_i}$, and α_Q the degree associated to the polytope Q .

As in the homogeneous case, one can consider the Koszul complex $Kos(S', F'_1, \dots, F'_k)$, and its graded pieces determined by the Chow group of X_{P+Q} . The following is our generalization of Theorem 1 to the sparse setting:

Theorem 3. *If P is n -dimensional, for any vertex v of $P + Q$, $Kos(S', F'_1, \dots, F'_k)_{\alpha_v + \alpha_P + \alpha_Q}$ is exact as a complex of K -vector spaces if and only if there are no common zeroes of $F_1, \dots, F_k$ in X_P .*

To generalize Theorem 2, set

$$(5) \quad f_i^g := \sum_{a \in \mathcal{A}_i} c_{i,a} t^a, \quad 1 \leq i \leq n+1,$$

with $c_{i,a}$ being new indeterminates. As before, we denote here with $\mathbb{K}$ the field $\mathbb{Q}(c_{i,a})$, and with $S'_{\mathbb{K}} := \mathbb{K}[x_1, \dots, x_{n+r}]$, the homogeneous coordinate ring of X_{P+Q} .

Associated with this data there is a *sparse resultant* ([GKZ94, CLO05]) which we will denote with $\text{Res}_{\mathcal{A}_1, \dots, \mathcal{A}_{n+1}} \in \mathbb{Z}[c_{i,a}]$. The main property of this polynomial is that if it is not identically 1, then it vanishes under a specialization of $f_i^g \mapsto f_i \in K[t^{\pm 1}]$ if and only if the homogenized system $F_1, \dots, F_{n+1} \in S$ made from $f_1, \dots, f_{n+1}$ with respect to $P_1, \dots, P_{n+1}$ respectively, has a non trivial solution in X_P .

Denote with $F_1^g, \dots, F_{n+1}^g \in S'$ the homogenizations of (5) to the coordinate ring of X_{P+Q} . For any degree β , we have that $Kos(S'_{\mathbb{K}}, F_1^g, \dots, F_{n+1}^g)_{\beta}$ is a complex of finite dimensional $\mathbb{K}$ -vector spaces, each of them being either trivial or having a monomial basis.

Theorem 4. Let $f_1^g, \dots, f_{n+1}^g$ be as in (5), and $F_1^g, \dots, F_{n+1}^g$ their respective P_i -homogenizations, $1 \leq i \leq n+1$. If P is n -dimensional and Q any integral polytope, for any vertex v of $P+Q$, $\text{Kos}(S'_{\mathbb{K}}, F_1^g, \dots, F_{n+1}^g)_{\alpha_v + \alpha_P + \alpha_Q}$ is exact as a complex of $\mathbb{K}$ -vector spaces. Moreover:

- (1) Up to a nonzero element in $\mathbb{Q}$, the determinant of $\text{Kos}(S'_{\mathbb{K}}, F_1^g, \dots, F_{n+1}^g)_{\alpha_v + \alpha_P + \alpha_Q}$ is equal to $\text{Res}_{\mathcal{A}_1, \dots, \mathcal{A}_{n+1}}$.
- (2) Up to a sign, $\text{Res}_{\mathcal{A}_1, \dots, \mathcal{A}_{n+1}}$ is equal to the gcd in $\mathbb{Q}[c_{i,a}]$ of the maximal minors of $\Psi_{1, \alpha_v + \alpha_Q + \alpha_P}$, the last nontrivial map of $\text{Kos}(S'_{\mathbb{K}}, F_1^g, \dots, F_{n+1}^g)_{\alpha_v + \alpha_P + \alpha_Q}$.
- (3) Let K be any field. For sparse polynomials $f_1, \dots, f_{n+1} \in K[t^{\pm 1}]$ of supports $\mathcal{A}_1, \dots, \mathcal{A}_{n+1}$ respectively, such that $\text{Res}_{\mathcal{A}_1, \dots, \mathcal{A}_{n+1}} \neq 1$, denote with $F_1, \dots, F_{n+1}$ their P_i -homogenizations, $1 \leq i \leq n+1$. Then, $\text{Kos}(S'_K, F_1, \dots, F_{n+1})_{\alpha_v + \alpha_P + \alpha_Q}$ is exact if and only if $\text{Res}_{\mathcal{A}_1, \dots, \mathcal{A}_{n+1}}(f_1, \dots, f_{n+1}) \neq 0$.

Remark 5. The degree α_v in the grading of the Koszul complex in Theorem 4 generalises the “ $-n$ ” in the degree $d_1 + \dots + d_{n+1} - n$ appearing in Theorem 2. In addition, all Canny-Emiris type matrices ([CE93, DJS23]) for the resultant can be regarded as non singular maximal square submatrices of the last map of the $(\alpha_v + \alpha_P)$ -th graded part of (2), where v is the vertex where the “perturbation” small generic vector $\delta \in \mathbb{Q}^n$ attains its minimum. The effective degree α_Q added corresponds to another polytope Q , which also produces a generalized Canny-Emiris type matrix as in [DJS23, Remark 4.28].

Remark 6. Theorem 4 gives a positive answer to Remark 4.20 in [DJS23] and it is independent of the results in that paper. So, it provides a simplification to the approach of proving Canny-Emiris’ conjecture for computing $\text{Res}_{\mathcal{A}_1, \dots, \mathcal{A}_{n+1}}$ as a quotient of two determinants.

REFERENCES

- [CE93] Canny, John; Emiris, Ioannis. *An efficient algorithm for the sparse mixed resultant*. Applied algebra, algebraic algorithms and error-correcting codes (San Juan, PR, 1993), 89–104, Lecture Notes in Comput. Sci., 673, Springer, Berlin, 1993.
- [Cha93] Chardin, Marc. *The resultant via a Koszul complex*. Computational algebraic geometry (Nice, 1992), 29–39, Progr. Math., 109, Birkhäuser Boston, Boston, MA, 1993.
- [CLO05] Cox, David A.; Little, John; O’Shea, Donal. *Using algebraic geometry*. Second edition. Graduate Texts in Mathematics, 185. Springer, New York, 2005.
- [DJS23] D’Andrea, Carlos; Jeronimo, Gabriela; Sombra, Martín. *The Canny-Emiris Conjecture for the Sparse Resultant*. Found. Comput. Math. 23 (2023), no. 3, 741–801.
- [Dem84] Demazure, Michel. *Une définition constructive du résultant*. Notes informelles de calcul formel. Prépublication du Centre de Mathématiques de l’Ecole Polytechnique, 1984.
- [GKZ94] Gel’fand, Izrail’ M.; Kapranov, Mikhail. M.; Zelevinsky, Andrey V. *Discriminants, resultants, and multidimensional determinants*. Mathematics: Theory & Applications. Birkhäuser Boston, Inc., Boston, MA, 1994.

Departament de Matemàtiques i Informàtica, Universitat de Barcelona. Gran Via 585, 08007 Barcelona, Spain & Centre de Recerca Matemàtica, Edifici C, Campus Bellaterra, 08193 Bellaterra, Spain

Email address: cdandrea@ub.edu

Departamento de Matemática, FCEN, Universidad de Buenos Aires, Ciudad Universitaria - Pab. I, (1428) Buenos Aires, Argentina, and CONICET-Universidad de Buenos Aires, Instituto de Investigaciones Matemáticas “Luis A. Santaló” (IMAS), Buenos Aires, Argentina

Email address: jeronimo@dm.uba.ar

UPPER BOUNDS FOR THE HOMOLOGY OF $K(\mathbb{Z}, n)$ AND $K(\mathbb{Z}/m\mathbb{Z}, n)$

JUAN ANTONIO DELGADO, ANA ROMERO, JULIO RUBIO AND FRANCIS SERGERAERT

ABSTRACT. In this work, we present closed explicit and numerical formulas for the number of critical simplices of two families of acyclic discrete vector fields on the Eilenberg-MacLane spaces $K(\mathbb{Z}, n)$ and $K(\mathbb{Z}/m\mathbb{Z}, n)$. As a consequence, these formulas will provide upper bounds for the number of components of the integral homology of these spaces.

INTRODUCTION

Throughout these notes we will work on a simplicial context, so we refer the reader to [9] for further details.

An *acyclic (or admissible) discrete vector field* V on a simplicial set X is a collection of pairs of non-degenerate simplices $V = \{(\sigma_i, \tau_i)\}_{i \in I}$, where every pair (σ_i, τ_i) is called a *vector* and it consists of an n -simplex σ_i called *source* and an $(n+1)$ -simplex τ_i called *target*, every simplex appears at most once in V , σ_i must be a regular face of τ_i and every possible path that can be formed along the vectors has finite length; n is not necessarily constant, may depend on i . A simplex that does not appear in V is said to be *critical*. One of the main results of [5] is that V induces a reduction $\rho : C_*^N(X) \rightrightarrows C_*^N(X)^c$, where ρ is a particular type of chain equivalence between two chain complexes, which is one of the basic notions of the Effective Homology Theory, see [13], and $C_*^N(X)^c$ is the V -reduced chain complex, which is generated by the critical simplices and is provided with an appropriate differential.

For the rest of this work, let π be a cyclic group. The simplicial model for the Eilenberg-MacLane spaces $K(\pi, n)$ for $n \geq 1$ consists of a large (or infinite) number of simplices. For this reason, the direct computation of the integral homology is difficult. In [3] we obtain results concerning acyclic discrete vector fields that allow us to compute the integral homology with generators of these spaces. We will introduce closed formulas, obtained experimentally due to our explicit computations, for the number of critical simplices of these acyclic vector fields. These formulas will provide us upper bounds for the integral homology of aforementioned spaces.

1. DISCRETE VECTOR FIELDS ON $K(\mathbb{Z}, n)$ AND $K(\mathbb{Z}/m\mathbb{Z}, n)$

The following two results are the starting points of our work. Let $m \geq 2$ be a positive integer.

Proposition 1.1. [8] *Let $V_{K(\mathbb{Z}, 1)}$ be defined as follows: the only critical simplices are the 0-simplex $\star$ and the 1-simplex $[1]$, the source simplices are the n -simplices $[a_{n-1}, \dots, a_0]$ with $a_{n-1} \neq 1$ and their corresponding target simplices are the $(n+1)$ -simplices*

Supported by grants PID2020-116641GB-I00 and PID2020-115225RB-I00 funded by MCIN/ AEI/ 10.13039/501100011033.

The talk at the meeting EACA 2024 has been given by the first author.

$[1, a_{n-1} - 1, a_{n-2}, \dots, a_0]$ if $a_{n-1} > 0$ and $[1, a_{n-1}, a_{n-2}, \dots, a_0]$ if $a_{n-1} < 0$. Then $V_{K(\mathbb{Z}, 1)}$ is an acyclic discrete vector field on $K(\mathbb{Z}, 1)$.

Proposition 1.2. [12] Let $V_{K(\mathbb{Z}/m\mathbb{Z}, 1)}$ be defined as follows: the critical simplices are the 0-simplex $\star$, the $2k$ -simplex $[m - 1, 1, \dots, m - 1, 1]$ for each $k \geq 1$ and the $(2k + 1)$ -simplex $[1, m - 1, 1, \dots, m - 1, 1]$ for each $k \geq 0$, the source simplices are the n -simplices $[a_{n-1}, \dots, a_{2r}, m - 1, 1, \dots, m - 1, 1]$ with $a_{2r} > 1$ and $0 \leq r \leq n/2$ and their corresponding target simplices are the $(n + 1)$ -simplices $[a_{n-1}, \dots, a_{2r} - 1, 1, m - 1, 1, \dots, m - 1, 1]$. Then $V_{K(\mathbb{Z}/m\mathbb{Z}, 1)}$ is an acyclic discrete vector field on $K(\mathbb{Z}/m\mathbb{Z}, 1)$.

Note that $V_{K(\mathbb{Z}/m\mathbb{Z}, 1)}$ has the same number of critical simplices for every $m \geq 2$; however, the homology groups are different. For this reason, we assert that our upper bound will not be the most precise one as it will not take account of m . The following result establishes an acyclic discrete vector field on BG , the classifying space of a simplicial group G .

Theorem 1.3. [3] Let G be a reduced simplicial group. Then there exists an acyclic discrete vector field on BG , denoted by V_{BG} , that induces a reduction $\rho : C_*^N(BG) \rightrightarrows \text{Bar}^{C_*^N(G)}(\mathbb{Z}, \mathbb{Z})$, where $\text{Bar}^{A_*}(\mathbb{Z}, \mathbb{Z})$ denotes the usual bar construction of a connected algebra A_* .

This result can be enhanced when we have an additional acyclic discrete vector field V_G on the reduced group G . We work as follows: we know that π is Abelian so, as a consequence, $K(\pi, n)$ is always a reduced Abelian simplicial group that can be constructed by means of the classifying space functor, that is, $K(\pi, n) = B(K(\pi, n - 1))$ for every $n \geq 1$. In this way, combining Proposition 1.1 and Proposition 1.2, for the infinite and finite case, respectively, together with the enhancement of Theorem 1.3, we obtain a family of acyclic discrete vector fields that we will denote by $V_{K(\mathbb{Z}, n)}$ and $V_{K(\mathbb{Z}/m\mathbb{Z}, n)}$, respectively, for every $n \geq 1$.

All of the previous results of this section lead up to algorithms that have been implemented in the computer algebra system Kenzo [4].

2. FORMULAS FOR THE NUMBER OF CRITICAL SIMPLICES

Let V be an acyclic discrete vector field on a simplicial set X . We define the *associated f -sequence*, and denote it by $c_f(V)$, as the sequence whose components are the number of critical simplices at each dimension. Let $\beta_k(X) := \text{Rank}(H_k(X; \mathbb{Z}))$ be the k -th Betti number of X and $t_k(X)$ the k -th torsion number, defined as the number of torsion groups of the invariant factor decomposition of $H_k(X; \mathbb{Z})$. Let us define $h_k(X)$ as $h_k(X) := \beta_k(X) + t_k(X)$. It is clear that, for every $k \geq 0$, $h_k(X) \leq c_f(V)_k$. This will be the upper bound that we will consider.

We present in Table 1 and Table 2 the first terms of the associated f -sequences of the acyclic discrete vector fields $V_{K(\mathbb{Z}, n)}$ and $V_{K(\mathbb{Z}/m\mathbb{Z}, n)}$ computed with our Kenzo programs. We recall that the f -sequences of $V_{K(\mathbb{Z}/m\mathbb{Z}, n)}$ do not depend on m .

The following results provide closed recursive formulas for the previous sequences. Let $n \geq 2$ be a positive integer.

Proposition 2.1. The k -th term of $c_f(V_{K(\mathbb{Z}, n)})$ is $\mathcal{P}_k^n$, where $\mathcal{P}_k^n$ is the k -th term of the n -th generalized Padovan sequence defined as follows: $\mathcal{P}_0^n = 1$ and $\mathcal{P}_1^n = \dots = \mathcal{P}_{n-1}^n = 0$ with the recurrence relation $\mathcal{P}_k^n = \mathcal{P}_{k-2}^n + \dots + \mathcal{P}_{k-n}^n$ for $k \geq n$.

$c_f(V_{K(\mathbb{Z},1)})$	1	1	0	0	0	0	0	0	0	0	0	0	0
$c_f(V_{K(\mathbb{Z},2)})$	1	0	1	0	1	0	1	0	1	0	1	0	1
$c_f(V_{K(\mathbb{Z},3)})$	1	0	0	1	0	1	1	1	2	2	3	4	5
$c_f(V_{K(\mathbb{Z},4)})$	1	0	0	0	1	0	1	1	2	2	4	5	8
$c_f(V_{K(\mathbb{Z},5)})$	1	0	0	0	0	1	0	1	1	2	3	4	7

TABLE 1. First terms of $c_f(V_{K(\mathbb{Z},n)})$ for $1 \leq n \leq 5$.

$c_f(V_{K(\mathbb{Z}/m\mathbb{Z},1)})$	1	1	1	1	1	1	1	1	1	1	1	1	1
$c_f(V_{K(\mathbb{Z}/m\mathbb{Z},2)})$	1	0	1	1	2	3	5	8	13	21	34	55	89
$c_f(V_{K(\mathbb{Z}/m\mathbb{Z},3)})$	1	0	0	1	1	2	4	7	13	24	44	81	149
$c_f(V_{K(\mathbb{Z}/m\mathbb{Z},4)})$	1	0	0	0	1	1	2	4	8	15	29	56	108
$c_f(V_{K(\mathbb{Z}/m\mathbb{Z},5)})$	1	0	0	0	0	1	1	2	4	8	16	31	61

TABLE 2. First terms of $c_f(V_{K(\mathbb{Z}/m\mathbb{Z},n)})$ for $1 \leq n \leq 5$.

Proposition 2.2. *The k -th term of $c_f(V_{K(\mathbb{Z}/m\mathbb{Z},n)})$ is 1 if $k = 0$ and $\mathcal{F}_k^n$ if $k > 0$, where $\mathcal{F}_k^n$ is the k -th term of the n -th generalized Fibonacci sequence defined as follows: $\mathcal{F}_1^n = \dots = \mathcal{F}_{n-1}^n = 0$ and $\mathcal{F}_n^n = 1$ with the recurrence relation $\mathcal{F}_k^n = \mathcal{F}_{k-1}^n + \dots + \mathcal{F}_{k-n}^n$ for $k > n$.*

The proof of Proposition 2.1 is deduced from [10] together with the enhancement of Theorem 1.3 and the proof of Proposition 2.2 is a reinterpretation of the fact that the k -th term of the n -th generalized Fibonacci generalized sequence is the number of compositions of $k - n + 1$ with no part greater than n , see [11]. As we have closed recursive expressions, we can provide general numerical formulas for the k -th term of these two families of sequences. We omit the trivial cases.

Proposition 2.3. *Let $n \geq 3$ and $k \geq 0$ be two integers. Then,*

- $\mathcal{P}_k^n$ is given by the following formula: $\mathcal{P}_k^n = \sum_{i=1}^n q_n(\lambda_i) \lambda_i^{k-n+2}$, where $\{\lambda_i\}_{1 \leq i \leq n}$ are the roots of the characteristic polynomial $\Phi_{\mathcal{P}_n}(x) = x^n - x^{n-2} - \dots - x - 1$, and $q_n(x) := \frac{x^n - x^{n-1} - x^{n-2} + 1}{(n+1)x^2 - nx - n + 1}$.
- the error function $\mathcal{E}_k^n := \mathcal{P}_k^n - q_n(\lambda) \lambda^{k-n+2}$, where λ is the dominant root of $\Phi_{\mathcal{P}_n}(x)$, satisfies $\lim_{k \rightarrow \infty} \mathcal{E}_k^n = 0$.

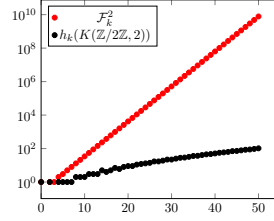
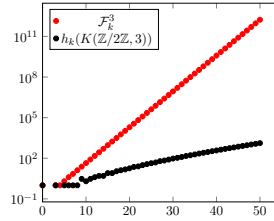
Proposition 2.4. *Let $n \geq 2$ and $k \geq 0$ be two integers. Then $\mathcal{F}_k^n = \left\lfloor \frac{\lambda^{k-1}(\lambda - 1)}{(n+1)\lambda - 2n} \right\rfloor$, where $\lfloor x \rfloor$ denotes the closest integer function and λ is the dominant root of the characteristic Laurent polynomial $\Phi_{\mathcal{F}_n}(x) = x + x^{-n} - 2$.*

The proof of Proposition 2.3 is obtained adapting the main results of [1, 7] to our particular Padovan sequences. The proof of Proposition 2.4 is first discussed in [6].

We end up this work comparing in Figure 1 and Figure 2 our upper bounds with the exact computations of the homology groups given in [2] for $h_k(K(\mathbb{Z}/2\mathbb{Z}, 2))$ and $h_k(K(\mathbb{Z}/2\mathbb{Z}, 3))$.

REFERENCES

- [1] J. J. Bravo and J. L. Herrera. Generalized Padovan sequences. *Communications of the Korean Mathematical Society*, 37(4):977-988, 2022.

FIGURE 1. Comparison between $\mathcal{F}_k^2$ and $h_k(K(\mathbb{Z}/2\mathbb{Z}, 2))$.FIGURE 2. Comparison between $\mathcal{F}_k^3$ and $h_k(K(\mathbb{Z}/2\mathbb{Z}, 3))$.

- [2] A. Clément. Integral Cohomology of Finite Postnikov Towers. Thèse de doctorat, Université de Lausanne, 2002.
- [3] J. A. Delgado, A. Romero, J. Rubio and F. Sergeraert. Discrete vector fields on the simplicial classifying space. Work in progress, 2024.
- [4] X. Dousson, J. Rubio, F. Sergeraert and Y. Siret. The Kenzo program. Institute Fourier, Grenoble, <https://www-fourier.ujf-grenoble.fr/~sergerar/Kenzo/>, 1999.
- [5] R. Forman. Morse Theory for Cell Complexes. *Advances in Mathematics*, 134(1):90-145, 1998.
- [6] M. Gardner. *The 2nd Scientific American Book of Mathematical Puzzles and Diversions, a New Selection*. University of California, Oakland, 1961.
- [7] V. Iliopoulos. The plastic number and its generalized polynomial. *Congent Mathematics*, 2(1), 2015.
- [8] M. Krčál, J. Matoušek and F. Sergeraert. Polynomial-time homology for simplicial Eilenberg-MacLane spaces. *Foundations of Computational Mathematics*, 13(6):935-963, 2013.
- [9] J. P. May. *Simplicial Objects in Algebraic Topology*. University of Chicago Press, Chicago, 1967.
- [10] R. Mullen. On determining paint by numbers puzzles with nonunique solutions. *Journal of Integer Sequences*, 12(6), 2009.
- [11] OEIS Foundation Inc. The On-Line Encyclopedia of Integer Sequences. Published electronically at <https://oeis.org>, 2024.
- [12] A. Romero. Effective homology and discrete Morse theory for the computation of homology of groups. Conference talk at *Maths, Algorithms and Proofs*, Logroño, 2010.
- [13] F. Sergeraert. The computability problem in Algebraic Topology. *Advances in Mathematics*, 104(1):1-29, 1994.

Universidad de La Rioja

Email address: {juan-antonio.delgado, ana.romero, julio.rubio}@unirioja.es

Université Grenoble-Alpes

Email address: francis.sergeraert@univ-grenoble-alpes.fr

FROBENIUS ALGEBRAS OF RINGS OF PRIME CHARACTERISTIC: A QUICK TOUR

ALBERTO F. BOIX AND DANNY A. J. GÓMEZ-RAMÍREZ

ABSTRACT. The goal of this survey is to review several recent results concerning the so-called Frobenius algebras of rings of prime characteristic, focusing specially on the interesting issue of its finite or infinite generation. We specially draw our attention to the case where our base ring is Stanley–Reisner, where explicit and algorithmic descriptions of these algebras are known.

INTRODUCTION

Let R be a commutative Noetherian ring of prime characteristic p , and let M be an R -module. For each integer $e \geq 0$, we denote by $\text{End}_{p^e}(M)$ the set of p^e -linear maps of M ; that is, $\text{End}_{p^e}(M)$ is made up by abelian group endomorphisms $M \xrightarrow{\phi} M$ such that

$$\phi(rm) = r^{p^e} \phi(m) \text{ for all } (r, m) \in R \times M.$$

In this way, one can cook up the so-called Frobenius algebra of M

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

where multiplication is given by composition of maps. This algebra, introduced in [LS01] in the context of tight closure theory has attracted some attention in the last years. In [LS01] it was raised the question of when these algebras were finitely generated as rings over its degree zero piece. They show that, if $M = R$ and $R \xrightarrow{F} R$ denotes the Frobenius endomorphism of R , then $\mathcal{F}^R \cong R[\Theta; F]$, see [LS01, Example 3.6]. The same conclusion holds when $(R, \mathfrak{m})$ is a local complete S_2 -ring, $M = H_{\mathfrak{m}}^{\dim(R)}(R)$ is the top local cohomology module of R supported on $\mathfrak{m}$, and F denotes the natural Frobenius action on this module [LS01, Example 3.7]. It is also known that $\mathcal{F}^M$ is finitely generated when M is of finite length [EY16, Theorem 2.11].

The goal of this paper is to survey some results concerning these algebras, focusing specially on the positive and negative answers that have appeared in the last years concerning its finite generation.

Date: April 24, 2024.

2020 Mathematics Subject Classification. Primary 13A35; Secondary 13F55.

Key words and phrases. Frobenius algebra, Frobenius map, Prime characteristic.

Alberto F. Boix is partially supported by Spanish Ministerio de Economía y Competitividad grant PID2022-137283NB-C22. He will present this work along the meeting.

1. ABOUT THE GENERATION OF FROBENIUS ALGEBRAS

It is in general quite complicated to obtain explicit descriptions of Frobenius algebras. One very important exception is the following result, which is known as Fedder's Lemma [Fed83].

Lemma 1.1. *Let $(R, \mathfrak{m})$ be a commutative Noetherian complete regular local ring of prime characteristic p , let $I \subset R$ be an ideal, and set $S := R/I$. Now, consider*

$$\mathcal{G}^S = \bigoplus_{e \geq 0} \left(\frac{(I^{[p^e]} :_R I)}{I^{[p^e]}} \right) F^e,$$

where F^e denotes the e -th iteration of the Frobenius map on the injective hull of the residue field of R . Then, we have a graded ring isomorphism $\mathcal{F}^{E_S} \cong \mathcal{G}^S$, where E_S denotes the injective hull of the residue field of S .

Thanks mainly to Fedder's Lemma, in [ÀMBZ12, ÀMY14] it is obtained a complete answer to the finite generation of Frobenius algebras in the Stanley–Reisner case. Recall that, given a commutative ring R of prime characteristic p and $v \in R$, $R[v\Theta; F]$ denotes the non-commutative ring freely generated as left R -module by $\{(v\Theta)^i\}_{i \geq 0}$ with the multiplication $(v\Theta) \cdot r = (vr^p)\Theta$.

Theorem 1.2. *Let $R = \mathbb{K}[[x_1, \dots, x_n]]/I$, where $\mathbb{K}$ is a field of prime characteristic p , and I is a squarefree monomial ideal. If $M = E_R$ is the injective hull of the residue field of R , then $\mathcal{F}^M$ is either infinitely generated or $\mathcal{F}^M \cong R[u\Theta; F]$, for some $u \in R$.*

Keeping in mind Theorem 1.2, it was natural to ask whether the finite/infinite generation of the Frobenius algebra attached to a Stanley–Reisner ring can be read in the simplicial complex given by the Stanley–Reisner correspondence. We give an answer to this question in the next section.

2. FROBENIUS ALGEBRAS, FREE FACES AND MAXIMAL FREE PAIRS

Let Δ be a simplicial complex with n vertices, we say that a pair (F, G) of non-empty, disjoint faces of Δ is **free** provided $F \cup G$ is the intersection of all the facets containing F . Moreover, given two free pairs $(F, G), (F', G')$, we say that $(F, G) \leq (F', G')$ if $F \supseteq F'$ and $G \subseteq G'$; with this partial order, the set of all the free pairs becomes a partially ordered set. In this way, a free pair (F, G) is said to be **maximal** if it is maximal in the set of free pairs with this order relation. On the other hand, let K be a field, let $I \subseteq K[x_1, \dots, x_n] = R$ be the squarefree monomial ideal attached to Δ through the Stanley–Reisner correspondence, and denote by $I^{[2]}$ the ideal obtained after raising to the square all the elements of I ; moreover, denote by J_1 the smallest ideal of R containing the set $(I^{[2]} :_R I) \setminus (I^{[2]} + (x_1 \cdots x_n))$. Finally, given a monomial $m \in R$, we denote by $\text{supp}(m)$ its support and by $\text{supp}_2(m)$ the set of indices i such that $\deg_{x_i}(m) = 2$. Keeping in mind all the above notations, the main result of this section (see [BZ19]) is the following theorem:

Theorem 2.1. *On the one hand, given a free pair (F, G) as above, set*

$$A(F, G) := \left(\prod_{i \in F} x_i^2 \right) \left(\prod_{i \notin F \cup G} x_i \right).$$

On the other hand, given a monomial $m \in R$ set $Y(m) := (\text{supp}_2(m), [n] \setminus \text{supp}(m))$. Then, the set $\{A(F, G) : (F, G) \text{ maximal free pair of } \Delta\}$ is the minimal monomial generating set for J_1 . Moreover, A and Y define 1 – 1 correspondences between the set of maximal free pairs of Δ and the set of minimal monomial generators of J_1 .

Apparently, Theorem 2.1 has no evident connection with the above Frobenius algebras. However, combining Theorem 2.1 jointly with the results obtained in [Ili20], we have:

Theorem 2.2. *Let K be any field of prime characteristic, let $R := K[[x_1, \dots, x_n]]$, let $I = I_\Delta \subseteq R$ be a squarefree monomial ideal, let $A := R/I$, and let E_A denote the injective hull of K as A -module. If $\mathcal{F}^{E_A}$ is infinitely generated as A -algebra, then the number of new generators appearing on each graded piece agree with the number of maximal free pairs of Δ .*

3. THE INFINITELY GENERATED LOCUS OF A FROBENIUS ALGEBRA

The question that motivates this section is the following one.

Question 3.1. *Let R be a commutative Noetherian ring of prime characteristic p . Is it true that $\{\mathfrak{p} \in \text{Spec}(R) : \mathcal{F}^{E_{\mathfrak{p}}}$ is finitely generated as a ring over its degree zero piece\} is an open set, where $E_{\mathfrak{p}}$ is the injective hull of the residue field of $R_{\mathfrak{p}}$?*

Before given a positive answer in the case of a Stanley–Reisner ring, we need to introduce the following notation. Given J a monomial ideal with minimal monomial generating set $\{m_1, \dots, m_r\}$, set $\text{LCM}_J := (\text{LCM}(m_i, m_j) : 1 \leq i < j \leq r)$. Moreover, given $F \subset \Delta$ a face, we set

$$\mathbf{x}_F = \prod_{i \in F} x_i.$$

In [BGRZ24] we prove the following result.

Theorem 3.2. *Let $\mathbb{K}$ be a field of prime characteristic p , let $R = \mathbb{K}[x_1, \dots, x_n]$, $S = R/I$, and I is a squarefree monomial ideal. Then, the set*

$$\{\mathfrak{p} \in \text{Spec}(R) : \mathfrak{p} \supseteq I, \mathcal{F}^{E_{S_{\mathfrak{p}}}} \text{ is not finitely generated as a ring over } \widehat{S_{\mathfrak{p}}}\}$$

is equal to $V(J)$, where

$$J = \bigcap_{F \in \text{IGL}(\Delta)} \mathfrak{p}_F,$$

$\mathfrak{p}_F$ is the prime ideal generated by the variables whose indices are not in F , and

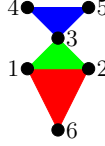
$$\text{IGL}(\Delta) := \{F \subset \Delta : (K^{[2]} :_R K) \neq K^{[2]} + \langle \text{LCM}_K \rangle, K := (I :_R \mathbf{x}_F)\}.$$

Theorem 3.2 leads to an algorithm, implemented in Macaulay2 [GS13], for computing the infinitely generated locus of the Frobenius algebra attached to a Stanley–Reisner ring.

- (i) **Step 1:** Initialize K as I , $\mathfrak{p}$ as the ideal $(x_1, \dots, x_n)$, and L as the empty list.
- (ii) **Step 2:** If $(K^{[2]} : K) \neq K^{[2]} + \langle \text{LCM}_K \rangle$, then add $\mathfrak{p}$ to the list L . Otherwise, return the empty list.
- (iii) **Step 3:** For each $\emptyset \neq F \subset \Delta$, assign to K the value $(I : \mathbf{x}_F)$. If $(K^{[2]} : K) \neq K^{[2]} + \langle \text{LCM}_K \rangle$, then add $\mathfrak{p} = \mathfrak{p}_F$ to the list L .
- (iv) **Step 4:** Output the intersection of the elements of L .

We finish by illustrating the above algorithm in a concrete example, borrowed from [BGRZ24].

Example 3.3. Let Δ be the simplicial complex given by facets $\{1, 2, 3\}$, $\{1, 2, 6\}$ and $\{3, 4, 5\}$, see the following figure.



We use our method to determine the non-finitely generated locus as follows.

```
loadPackage "SimplicialComplexes";

load "non_finitely_generated_locus_algorithm.m2";

R=QQ[x,y,z,w,a,b];

A= simplicialComplex {x*y*z,x*y*b,z*w*a};

I=monomialIdeal(A);

nonfglocus(I)

monomialIdeal (x, y, w, a, b)
```

REFERENCES

- [ÁMBZ12] J. Álvarez Montaner, A. F. Boix, and S. Zarzuela. Frobenius and Cartier algebras of Stanley-Reisner rings. *J. Algebra*, 358:162–177, 2012.
- [ÁMY14] J. Álvarez Montaner and K. Yanagawa. Addendum to “Frobenius and Cartier algebras of Stanley-Reisner rings” [J. Algebra 358 (2012) 162–177]. *J. Algebra*, 414:300–304, 2014.
- [BGRZ24] A. F. Boix, D. A. J. Gómez-Ramírez, and S. Zarzuela. On the infinitely generated locus of Frobenius algebras of rings of prime characteristic. *Acta Math. Vietnam.*, 2024. <https://doi.org/10.1007/s40306-023-00515-3>.
- [BZ19] A. F. Boix and S. Zarzuela. Frobenius and Cartier algebras of Stanley-Reisner rings (II). *Acta Math. Vietnam.*, 44(3):571–586, 2019.
- [EY16] F. Enescu and Y. Yao. The Frobenius complexity of a local ring of prime characteristic. *J. Algebra*, 459:133–156, 2016.
- [Fed83] R. Fedder. F -purity and rational singularity. *Trans. Amer. Math. Soc.*, 278(2):461–480, 1983.
- [GS13] Daniel R. Grayson and Michael E. Stillman. Macaulay2, a software system for research in algebraic geometry. Available at <http://www.math.uiuc.edu/Macaulay2/>, 2013.
- [Ili20] I. Ilioaia. On the Frobenius complexity of Stanley-Reisner rings. *Comm. Algebra*, 48(10):4176–4185, 2020.
- [LS01] G. Lyubeznik and K. E. Smith. On the commutation of the test ideal with localization and completion. *Trans. Amer. Math. Soc.*, 353(8):3149–3180 (electronic), 2001.

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

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

Area of Fundamental Sciences, EAFIT University, Medellín, Colombia.

Email address: daj.gomezramirez@gmail.com

DISTRIBUTED MATRIX MULTIPLICATION OVER SMALL FIELDS WITH STRAGGLER TOLERANCE

ADRIÁN FIDALGO-DIAZ AND UMBERTO MARTÍNEZ-PEÑAS

ABSTRACT. A distributed algorithm scales poorly when the number of nodes is large, due to the difference in their execution times (the straggler effect). We consider the problem of mitigating this effect in distributed matrix multiplication when the matrices are defined over a small finite field. For this purpose, we introduce a new algorithm based on evaluating polynomials in several variables, provide an explicit solution and study its optimality.

INTRODUCTION

In order to multiply large matrices, parallelization is used as follows to obtain feasible runtimes. The two matrices are subdivided into smaller blocks, in a way that the product of the two large matrices is obtained from the products of pairs of the smaller submatrices (see Section 2). A master node shares the smaller submatrices with a set of worker nodes and gathers all the results when finished. As the number of nodes grows, so does the expected difference between their execution times. Since the master node has to wait for every worker node to end their computations, this supposes a bottleneck that difficults an efficient scaling of this architecture. The solution comes from the hand of coding theory: consider the slowest nodes, the so called stragglers, as the erasures in a word of a code. With this idea, polynomial codes [3] were proposed inspired by Reed-Solomon codes.

In this paper we generalize polynomial codes [3] using multivariate polynomials, similarly to how Reed-Muller codes generalize Reed-Solomon codes. In this way, we increase the number of points where the polynomials can be evaluated, allowing to define algorithms that use a higher number of worker nodes than the size of the field. We study the case where the matrices are defined over $\mathbb{F}_2$, a field for which polynomial codes do not work and where there is a lack of optimal towers of algebraic function fields, thus making our previous construction [2] not applicable.

1. PRELIMINARIES. THE FOOTPRINT BOUND

We denote by $\mathbb{F}_q$ the finite field of size q and define the $\mathbb{F}_q$ -algebra

$$\mathcal{R} = \frac{\mathbb{F}_q[x_1, x_2, \dots, x_\ell]}{(x_1^q - x_1, \dots, x_\ell^q - x_\ell)},$$

The authors gratefully acknowledge the support from a María Zambrano contract by the University of Valladolid, Spain (Contract no. E-47-2022-0001486), and the support from MCIN/AEI/10.13039/501100011033 and the European Union NextGenerationEU/PRTR (Grant no. TED2021-130358B-I00).

The talk at the meeting EACA 2024 has been given by the first author.

where $(\mathcal{A})$ denotes the ideal generated by a set $\mathcal{A}$. Let $\mathcal{V} \subseteq \mathcal{R}$ be an $(\mathbb{F}_q$ -linear) vector subspace. For a set $\mathbb{P} \subseteq \mathbb{F}_q^\ell$, consider the evaluation map $ev : \mathcal{V} \rightarrow \mathbb{F}_q^\mathbb{P}$ which sends $f \in \mathcal{V}$ to $(f(P))_{P \in \mathbb{P}}$, its evaluations in $\mathbb{P}$. Observe that ev is well defined and a linear map.

For $f \in \mathbb{F}_q[x_1, x_2, \dots, x_\ell]$, we define its restricted footprint as $\Delta_{q, \prec}(f) := \{a \in \mathbb{N}_{< q}^\ell : x^a \notin (\text{LT}(f))\}$, where $\mathbb{N}_{< q} = \{0, 1, \dots, q-1\}$, $\prec$ is a monomial ordering (defined in $\mathbb{N}^\ell$), $x^a = x_1^{a_1} \cdots x_\ell^{a_\ell}$, for $a \in \mathbb{N}_{< q}^\ell$, and $\text{LT}(f)$ denotes the leading monomial of f with respect to $\prec$. The following lemma can be found in [1, Sec. IV].

Lemma 1.1. *Let $f \in \mathbb{F}_q[x_1, x_2, \dots, x_\ell]$ and $\delta(f) := |\Delta_{q, \prec}(f)|$. If $Z(f)$ denotes the set of zeros of f , then $|Z(f)| \leq \delta(f)$. In particular, if we define $\delta(\mathcal{V}) := \max\{\delta(f) : f \in \mathcal{V} \setminus \{0\}\}$, then $|Z(f)| \leq \delta(\mathcal{V})$, for all $f \in \mathcal{V} \setminus \{0\}$.*

As a consequence, denoting $k := \delta(\mathcal{V})$, if $f \in \mathcal{V}$ and $f(P_i) = 0$ for $k+1$ distinct points $P_1, P_2, \dots, P_{k+1} \in \mathbb{P}$, then $f = 0$. Equivalently, let $\mathcal{B} := \{f_1, f_2, \dots, f_\kappa\}$ be a basis of $\mathcal{V}$ and G be the matrix associated to ev in such a basis, that is,

$$(1) \quad G := \begin{pmatrix} f_1(P_1) & f_1(P_2) & \dots & f_1(P_{k+1}) \\ f_2(P_1) & f_2(P_2) & \dots & f_2(P_{k+1}) \\ \vdots & \vdots & \ddots & \vdots \\ f_\kappa(P_1) & f_\kappa(P_2) & \dots & f_\kappa(P_{k+1}) \end{pmatrix}.$$

Then G has a right inverse, i.e., ev is injective.

2. DISTRIBUTED MATRIX MULTIPLICATION. THE GENERAL CASE

Let $A \in \mathbb{F}_q^{r \times s}$ and $B \in \mathbb{F}_q^{s \times t}$ be matrices over $\mathbb{F}_q$. In order to multiply them, we split them as block matrices in the following way:

$$A := \begin{pmatrix} A_1 \\ A_2 \\ \vdots \\ A_m \end{pmatrix}, \quad B := (B_1 \ B_2 \ \dots \ B_n) \implies AB = \begin{pmatrix} A_1 B_1 & A_1 B_2 & \dots & A_1 B_n \\ A_2 B_1 & A_2 B_2 & \dots & A_2 B_n \\ \vdots & \vdots & \ddots & \vdots \\ A_m B_1 & A_m B_2 & \dots & A_m B_n \end{pmatrix},$$

where $A_i \in \mathbb{F}_q^{\frac{r}{m} \times s}$ and $B_i \in \mathbb{F}_q^{s \times \frac{t}{n}}$ (assuming that m and n divide r and t , respectively). We want to find $p_A \in \mathcal{R}^{\frac{r}{m} \times s}$ and $p_B \in \mathcal{R}^{s \times \frac{t}{n}}$ such that

$$p_A := \sum_{i=1}^m A_i x^{a_i}, \quad p_B := \sum_{i=1}^n B_i x^{b_i},$$

and such that, for every $a, a' \in D_A := \{a_1, \dots, a_m\} \subseteq \mathbb{N}_{< q}^\ell$ and $b, b' \in D_B := \{b_1, \dots, b_n\} \subseteq \mathbb{N}_{< q}^\ell$,

$$(2) \quad a + b = a' + b' \implies (a, b) = (a', b').$$

Here, we define the sum in $\mathbb{N}_{< q}$ as usual with the added rule $a + b := (a + b \bmod q) + 1$, for $a, b \in \mathbb{N}_{< q}$ such that $a + b > q$. Note that we still have $x^a x^b = x^{a+b}$ in $\mathcal{R}$ for all $a, b \in \mathbb{N}_{< q}^\ell$. Set $h := p_A p_B \in \mathcal{R}^{\frac{r}{m} \times \frac{t}{n}}$.

Remark 2.1. By enforcing (2) we ensure that $A_i B_j$ is the coefficient of the term of h with degree $a_i + b_j$, so we can retrieve AB from knowing h .

Observe that if $h_{i,j} \in \mathcal{R}$ is the (i,j) th coordinate of h , then $h_{i,j} \in \mathcal{V} := \langle x^{a+b} : a \in D_A, b \in D_B \rangle_{\mathbb{F}_q}$, where $\langle \cdot \rangle_{\mathbb{F}_q}$ denotes $\mathbb{F}_q$ -linear span. So from Section 1, we can interpolate h from any $k+1$ evaluations (the image of h from ev defined with $|\mathbb{P}| = k+1$), where $k = \delta(\mathcal{V})$, by inverting the matrix G from (1). Since $\mathcal{V}$ is generated by monomials, $\delta(\mathcal{V})$ is independent of the monomial ordering. This interpolation step has negligible computational complexity compared to that of each worker when the matrix sizes r, s and t are large, as in [2, Sec. 5].

This results in the following algorithm: the master node shares a point $P_i \in \mathbb{F}_q^\ell, p_A$ and p_B with each worker. Then, the workers compute $h(P_i) = p_A(P_i)p_B(P_i)$ in parallel. When any $k+1$ of them end, the master node recovers h by performing componentwise interpolations, and so AB because of Remark 2.1. In the literature, the number $k+1$ is called the recovery threshold, i.e., the minimum number of responsive nodes needed to recover the product AB .

The remaining part is how to select sets $D_A, D_B \subseteq \mathbb{N}_{<q}^\ell$ satisfying (2) in such way that k is as small as possible. Noticing that $\mathcal{V}$ is generated by monomials, we conclude that

$$(3) \quad k = \delta(\mathcal{V}) = q^\ell - \min \left\{ \prod_{i=1}^\ell (q - a_i) : x^a \in \mathcal{V} \right\}.$$

We summarize the problem of obtaining the coefficients of p_A and p_B satisfying (2) and minimizing (3) in Problem 1.

Problem 1. Find $D_A, D_B \subseteq \mathbb{N}_{<q}^\ell$ such that

- (1) $|D_A| = m$ and $|D_B| = n$,
- (2) $|D_A + D_B| = |D_A| \cdot |D_B|$ or, equivalently, satisfying (2), and
- (3) $\min\{\prod_{i=1}^\ell (q - a_i - b_i) : a \in D_A, b \in D_B\}$ is as large as possible.

Now the goal is solving Problem 1 since this leads to an optimal distributed matrix multiplication (DMM) algorithm (in the framework that we have defined).

Remark 2.2. In the case $\ell = 1$ (polynomials defined over one variable), this algorithm is known as polynomial codes [3] in the literature, and Problem 1 is solved by choosing $D_A := \{0, 1, \dots, m-1\}$ and $D_B := \{0, m, \dots, (n-1)m\}$. Polynomial codes attain the best information theoretical recovery threshold but the number of worker nodes is limited by the size of the field the matrices are defined over. In particular, small fields such as $\mathbb{F}_2$ or $\mathbb{F}_3$ are not allowed by polynomial codes [3].

3. MATRICES OVER $\mathbb{F}_2$

For the remainder of the paper we restrict ourselves to the case where A and B are defined over $\mathbb{F}_2$. When $q = 2$, Problem 1 is simplified. We have the following lower bound on the recovery threshold.

Proposition 3.1. Let $\xi := \min\{d \in \mathbb{N} : mn \leq \sum_{i=0}^d \binom{\ell}{i}\}$. Then

$$\min \left\{ \prod_{i=1}^\ell (2 - a_i - b_i) : a \in D_A, b \in D_B \right\} \leq 2^{\ell-\xi}.$$

Proof. Since $q = 2$, maximizing the minimum of Problem 1 is equivalent to minimizing $d := \max\{\text{wt}_H(a+b) : a \in D_A, b \in D_B\}$, where wt_H denotes the Hamming weight in

$\mathbb{N}_{<2}^\ell = \{0, 1\}^\ell$. This is because, when $q = 2$, it holds that

$$\prod_{i=1}^{\ell} (2 - a_i - b_i) = 2^{\ell - \text{wt}_H(a+b)},$$

due to the definition of the sum in $\mathbb{N}_{<2}$. Now, by item 2 in Problem 1, we have that

$$mn = |D_A + D_B| \leq |\{a \in \mathbb{N}_{<2}^\ell : \text{wt}_H(a) \leq d\}| = \sum_{i=0}^d \binom{\ell}{i}.$$

From the definition of ξ , we deduce the bound of the statement. $\square$

We next provide an explicit construction of D_A and D_B . In general, the recovery threshold of Construction 1 does not achieve the bound of Proposition 3.1. However, it does for some moderate values of ℓ , yielding interesting DMM algorithms as shown in Table 1.

Construction 1. Let $\ell = m' + n'$, $d_m \leq m'$ and $d_n \leq n'$. Consider

$$D_A := \{a \in \mathbb{N}_{<2}^\ell : \text{wt}_H(a) \leq d_m, \quad a_i = 0, \quad i = m' + 1, m' + 2, \dots, \ell\},$$

$$D_B := \{b \in \mathbb{N}_{<2}^\ell : \text{wt}_H(b) \leq d_n, \quad b_i = 0, \quad i = 0, 1, \dots, m'\}.$$

From the definition we get $|D_A + D_B| = |D_A||D_B|$ with

$$m := |D_A| = \sum_{i=0}^{d_m} \binom{m'}{i}, \quad n := |D_B| = \sum_{i=0}^{d_n} \binom{n'}{i}.$$

Its recovery threshold is $2^\ell - 2^{\ell - d_m - d_n}$.

ℓ	m, n	Number of workers	Recovery threshold
4	3	16	13
8	11	256	241
12	42	4096	4033
16	163	65536	65281

TABLE 1. Parameters for Construction 1 with $m' = n' = \ell/2$ and $d_m = d_n = \ell/4$ for some values of ℓ attaining the bound of Proposition 3.1.

REFERENCES

- [1] O. Geil, and T. Høholdt, “Footprints or generalized Bezout’s theorem,” *IEEE Transactions on information theory*, 46(2):635–641, 2000.
- [2] A. Fidalgo-Díaz and U. Martínez-Peñas, “Distributed matrix multiplication with straggler tolerance using algebraic function fields,” 2024, Preprint: arXiv:2401.13573.
- [3] Q. Yu, M. Maddah-Ali, and S. Avestimehr, “Polynomial codes: an optimal design for high-dimensional coded matrix multiplication,” *Advances in Neural Information Processing Systems*, 30:1–11, 2017.

University of Valladolid
Email address: `adrian.fidalgo22@uva.es`

University of Valladolid
Email address: `umberto.martinez@uva.es`

ON THE QUOTIENT OF $\mathcal{C}$ -SEMIGROUPS

J. I. GARCÍA-GARCÍA, R. TAPIA-RAMOS, AND A. VIGNERON-TENORIO

ABSTRACT. Let $S \subseteq \mathbb{N}^p$ (for some non-zero natural number p) be an affine semigroup, and $\mathcal{C} \subseteq \mathbb{N}^p$ be the non-negative integer cone generated by S . We say that S is a $\mathcal{C}$ -semigroup if the complement of S in $\mathcal{C}$ is finite. In this talk, we study the quotient of a $\mathcal{C}$ -semigroup by a positive integer, and we generalize several irreducibility results for the quotient of numerical semigroups to the quotient of a $\mathcal{C}$ -semigroup by a positive integer.

INTRODUCTION AND MOTIVATION

This work is based on [4]. Given an affine semigroup $S \subseteq \mathbb{N}^p$, its quotient by a positive integer d is defined as $\frac{S}{d} = \{x \in \mathbb{N}^p \mid dx \in S\}$. We say that $\frac{S}{2}$ is one-half of S , and that $\frac{S}{4}$ is one-fourth of S . These specific cases will be relevant later in the introduced results.

There are numerous papers about the quotient of numerical semigroups (when $p = 1$), such as [1], [5], and [7]. Recently, multiple studies have extended some well-known results about numerical semigroups to algebraic structures of higher dimensions, such as affine semigroups. Following this line of research, we generalize properties, and characterizations, known about quotients of numerical semigroups to quotients of $\mathcal{C}$ -semigroups. We point out that despite some of the results we present being known for numerical semigroups, others hold only for general $\mathcal{C}$ -semigroups.

One of our main objectives is to describe $\mathcal{C}$ -semigroups that are quotients of a given $\mathcal{C}$ -semigroup. Another key objective is to study the irreducibility of quotients of $\mathcal{C}$ -semigroups. In particular, we provide a characterization of irreducible $\mathcal{C}$ -semigroups relative to the quotient of $\mathcal{C}$ -semigroups.

For a $\mathcal{C}$ -semigroup S , any element $x \in \mathcal{C} \setminus S$ is called a gap of S . The set of all gaps in S is denoted by $\mathcal{H}(S)$ and its cardinality is known as the genus of S . Following these definitions, fixed $\preceq$ a total order on $\mathbb{N}^p$, the Frobenius element of S , denoted by $Fb_{\preceq}(S)$, is $\max_{\preceq}(\mathcal{C} \setminus S)$. Note that $Fb_{\preceq}(S)$ depends on the specific total order $\preceq$ chosen previously. Using the terminology given in [2], we say that $x \in \mathcal{H}(S)$ is a pseudo-Frobenius element if $x + (S \setminus \{0\}) \subset S$. The set of pseudo-Frobenius elements is denoted by $PF(S)$.

1. ELEMENTS OF $\mathcal{D}_d(S, f)$

Let S be a $\mathcal{C}$ -semigroup and $d \in \mathbb{N} \setminus \{0\}$. We define $\mathcal{D}_d(S)$ as the set of all the $\mathcal{C}$ -semigroups T such that $S = \frac{T}{d}$. Let $f = Fb_{\preceq}(T)$, with $T \in \mathcal{D}_d(S)$, notice that $f \succ dFb_{\preceq}(S)$, otherwise,

All the authors have been partially supported by Consejería de Universidad, Investigación e Innovación de la Junta de Andalucía project ProyExcel_00868 and research group FQM343. Proyectos de investigación del Plan Propio – UCA 2022-2023 (PR2022-011 and PR2022-004) partially supported the first, and third-named authors. The last author is partially supported by grant PID2022-138906NB-C21 funded by MICIU/AEI/10.13039/501100011033 and by ERDF/EU. The talk at the meeting EACA 2024 has been given by the second author.

for any $f \preceq x \preceq dFb_{\preceq}(S)$, if $\frac{x}{d} \in \mathbb{N}^p$ necessarily $\frac{x}{d} \in S$, which it is not possible since $x \preceq dFb_{\preceq}(S)$. Thus, the set $\mathcal{D}_d(S)$ is not finite since f can be any element belonging to $\mathcal{C}$ greater than $dFb_{\preceq}(S)$. But, fixed an element $f \succ dFb_{\preceq}(S)$, the set $\mathcal{D}_d(S, f) = \{T \in \mathcal{D}_d(S) \mid Fb_{\preceq}(T) \preceq f\}$ is finite and can be computed.

Given $X \subseteq \mathbb{N}^p$, let $dX = \{dx \mid x \in X\}$. The following algorithm, given in pseudocode form, shows a procedure to describe all the $\mathcal{C}$ -semigroups belonging to $\mathcal{D}_d(S, f)$. It is achieved as a consequence of [4, Theorem 12].

Algorithm 1: Computing $\mathcal{D}_d(S, f)$

Input: A $\mathcal{C}$ -semigroup S , a positive integer d , and $f \in \mathcal{C} \setminus \{0\}$.

Output: The set $\mathcal{D}_d(S, f)$.

```

1 if  $f \preceq dFb_{\preceq}(S)$  then
2   return  $\emptyset$ 
3  $M \leftarrow \{m \in S \setminus \mathbb{N}^p \mid m \preceq f\};$ 
4  $A \leftarrow \{1, 2, \dots, d-1\};$ 
5  $P \leftarrow \mathcal{P}(M) \setminus \{\emptyset\};$ 
6  $\mathcal{D} \leftarrow \{\{x \in \mathcal{C} \mid x \succ f\} \cup dS\};$ 
7 for  $\Lambda \in P$  do
8    $t \leftarrow \#\Lambda;$ 
9   if  $\sum_{i=1}^t a_i \lambda_i \in dS \sqcup (\mathbb{N}^p \setminus d\mathbb{N}^p)$ , for all  $\lambda_i \in \Lambda$ , and  $a_i \in A$  then
10     $T \leftarrow \{x \in \mathcal{C} \mid x \succ f\} \cup (dS + \{\sum_{i=1}^t a_i \lambda_i \mid \lambda_i \in \Lambda, a_i \in A\});$ 
11     $\mathcal{D} = \mathcal{D} \cup \{T\};$ 
12 return  $\mathcal{D}$ 
```

Example 1.1. Consider the non-negative integer cone $\mathcal{C}$ generated by $\{(2, 1), (3, 1), (4, 1), (9, 5)\}$ and the $\mathcal{C}$ -semigroup S minimally generated by

$$\{(4, 1), (5, 2), (7, 2), (9, 5), (4, 2), (6, 2), (6, 3), (7, 3), (11, 6)\}.$$

This semigroup is the non-negative integer cone $\mathcal{C}$ except the points $\{(2, 1), (3, 1)\}$ (see Figure 1). Fixed $d = 3$, $f = 3Fb_{\preceq}(S) = (9, 3)$, and the reverse graded lexicographical order. Figure 2 shows some graphical examples of elements belonging to $\mathcal{D}_3(S, f)$. The symbols "o" represent the gaps of the $\mathcal{C}$ -semigroup, and the red dots "•" the elements in the $\mathcal{C}$ -semigroup.

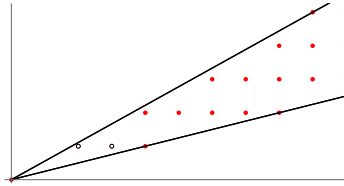
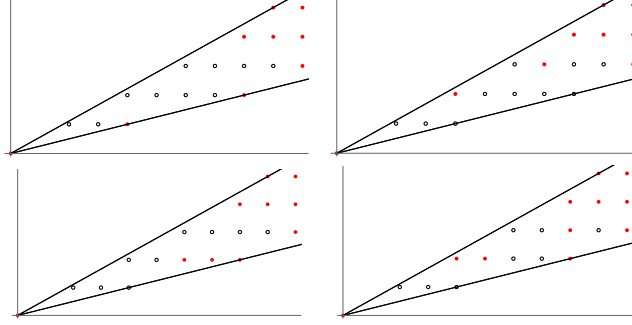


FIGURE 1. $\mathcal{C}$ -semigroup S ; $\circ \equiv$ gap, $\bullet \equiv$ element in S .

FIGURE 2. Some elements in $\mathcal{D}_3(S)$.

2. IRREDUCIBILITY

A $\mathcal{C}$ -semigroup S is irreducible if it cannot be expressed as an intersection of two $\mathcal{C}$ -semigroups containing S properly. Equivalently, S is irreducible if and only if the set $PF(S)$ is equal to $\{Fb_{\preceq}(S)\}$ or $\{Fb_{\preceq}(S), \frac{Fb_{\preceq}(S)}{2}\}$ (see [2]). If $PF(S) = \{Fb_{\preceq}(S)\}$, we say that S is symmetric, and pseudo-symmetric when $PF(S) = \{Fb_{\preceq}(S), \frac{Fb_{\preceq}(S)}{2}\}$.

The following results are inspired by [6], and by the study of the irreducibility of $\mathcal{C}$ -semigroups given in [2]. From now on, we denote by $\mathcal{O}$ the set $\mathbb{N} \setminus 2\mathbb{N}$ of odd non-negative integers.

Theorem 2.1. *Let S be a $\mathcal{C}$ -semigroup and $f \in \mathcal{C} \cap \mathcal{O}^p$ such that $f - f_i - f_j \in S$ for all $f_i, f_j \in PF(S) = \{f_1, \dots, f_t\}$. Then,*

$$\begin{aligned} T &= 2S \cup \{x \in \mathcal{C} \mid f - x \notin \mathcal{C}\} \\ &\cup \bigcup_{i=1}^t \left((f - 2f_i) + 2S \right) \\ &\cup \left\{ x \in \mathcal{C} \setminus (2\mathbb{N}^p \cup \mathcal{O}^p) \mid x \succ \frac{f}{2}, f - x \in \mathcal{C} \right\} \end{aligned}$$

is a symmetric $\mathcal{C}$ -semigroup, with Frobenius element f , and such that $S = \frac{T}{2}$.

Corollary 2.2. *Given a $\mathcal{C}$ -semigroup S there are infinitely many symmetric $\mathcal{C}$ -semigroups T such that $S = \frac{T}{2}$.*

There is not a parallelism between the symmetric and pseudo-symmetric cases. It means that if S is a $\mathcal{C}$ -semigroup there exists finitely many pseudo-symmetric $\mathcal{C}$ -semigroup T such that $S = \frac{T}{2}$. This is achieved as a consequence of that $Fb_{\preceq}(T) = 2Fb_{\preceq}(S)$. Since there exist finitely many $\mathcal{C}$ -semigroups with Frobenius element $2Fb_{\preceq}(S)$, we affirm that we cannot obtain a result similar for the pseudo-symmetric case. Whence, we obtain the following result.

Proposition 2.3. *Let T be a pseudo-symmetric $\mathcal{C}$ -semigroup. Then, $\frac{T}{2}$ is an irreducible $\mathcal{C}$ -semigroup.*

In particular, it is not true that any $\mathcal{C}$ -semigroup is one-half of a pseudo-symmetric $\mathcal{C}$ -semigroup. Moreover, we can sharpen the preceding result a bit further to distinguish which cases one-half of a pseudo-symmetric $\mathcal{C}$ -semigroup is symmetric or pseudo-symmetric.

Corollary 2.4. *Let T be a pseudo-symmetric $\mathcal{C}$ -semigroup and $S = \frac{T}{2}$. Then:*

- (1) *S is symmetric if and only if $Fb_{\preceq}(S) \not\equiv 0 \pmod{4}$.*
- (2) *S is pseudo-symmetric if and only if $Fb_{\preceq}(S) \equiv 0 \pmod{4}$.*

Since it is easy to check if $Fb_{\preceq}(S) \not\equiv 0 \pmod{4}$, the above result is a helpful tool to determine if S is symmetric or pseudo-symmetric. We now try to give a flavour towards the task of how to characterise irreducible $\mathcal{C}$ -semigroups relative to one-half of $\mathcal{C}$ -semigroups. First of all, we deal with a technical result.

Lemma 2.5. *Let S be an irreducible $\mathcal{C}$ -semigroup, $\preceq$ a monomial order and the set*

$$A = \{x \in (\mathbb{N}^p \setminus 2\mathbb{N}^p) \cap \mathcal{C} \mid Fb_{\preceq}(S) \prec x \prec 2Fb_{\preceq}(S)\}.$$

Then,

$$T = 2S \cup A \cup \{x \in \mathcal{C} \mid x \succ 2Fb_{\preceq}(S)\}$$

is a pseudo symmetric $\mathcal{C}$ -semigroup, with Frobenius element $2Fb_{\preceq}(S)$, and such that $S = \frac{T}{2}$.

Theorem 2.6. *Every $\mathcal{C}$ -semigroup is one-fourth of infinitely many pseudo-symmetric $\mathcal{C}$ -semigroups.*

Theorem 2.7. *A $\mathcal{C}$ -semigroup is irreducible if and only if it is one-half of a pseudo-symmetric $\mathcal{C}$ -semigroup.*

REFERENCES

- [1] Bogart, T.; O'Neill, C.; Woods, K., *When is a numerical semigroup a quotient?* Bull. Aust. Math. Soc.109(2024), no.1, 67–76.
- [2] García-García, J. I.; Marín-Aragón, D.; Sánchez-Loureiro, A.; Vigneron-Tenorio, A., *Some Properties of Affine $\mathcal{C}$ -semigroups*. Results Math, 79 (2024), no. 52.
- [3] García-García, J. I.; Marín-Aragón, D.; Vigneron-Tenorio A., *An extension of Wilf's conjecture to affine semigroups*, Semigroup Forum (2018), vol. 96, Issue 2, 396–408.
- [4] García-García, J. I.; Tapia-Ramos, R.; Vigneron-Tenorio, A., *On the quotient of affine semigroups by a positive integer*, 2024. arXiv preprint: <https://arxiv.org/abs/2402.09159>.
- [5] Ojeda, I.; Rosales, J. C., *The arithmetic extensions of a numerical semigroup*. Communications in Algebra, 48:9 (2020), 3707–3715.
- [6] Rosales, J. C.; García-Sánchez, P. A., Numerical Semigroups. Dev. Math., 20 Springer, New York, 2009.
- [7] Swanson, I., *Every numerical semigroup is one over d of infinitely many symmetric numerical semigroups*, Commutative algebra and its applications, 383–386. Walter de Gruyter GmbH & Co. KG, Berlin, 2009.

Universidad de Cádiz, E-11510 Puerto Real (Cádiz, Spain).

Email address: ignacio.garcia@uca.es

Universidad de Cádiz, E-11406 Jerez de la Frontera (Cádiz, Spain).

Email address: raquel.tapia@uca.es

Universidad de Cádiz, E-11406 Jerez de la Frontera (Cádiz, Spain).

Email address: alberto.vigneron@uca.es

BETTI NUMBERS OF PROJECTIVE AND AFFINE MONOMIAL CURVES

IGNACIO GARCÍA-MARCO, PHILIPPE GIMENEZ, AND MARIO GONZÁLEZ-SÁNCHEZ

ABSTRACT. In this work, we explore when the Betti numbers of the coordinate rings of a projective monomial curve and one of its affine projections are identical. Given an infinite field k and a sequence of relatively prime integers $a_0 = 0 < a_1 < \dots < a_n = d$, we consider the projective monomial curve $\mathcal{C} \subset \mathbb{P}_k^n$ of degree d parametrically defined by $x_i = u^{a_i} v^{d-a_i}$ for all $i \in \{0, \dots, n\}$ and its coordinate ring $k[\mathcal{C}]$. The curve $\mathcal{C}_1 \subset \mathbb{A}_k^n$ with parametric equations $x_i = t^{a_i}$ for $i \in \{1, \dots, n\}$ is an affine projection of $\mathcal{C}$ and we denote by $k[\mathcal{C}_1]$ its coordinate ring. The main contribution of this paper is the introduction of a novel (Gröbner-free) combinatorial criterion that provides a sufficient condition for the equality of the Betti numbers of $k[\mathcal{C}]$ and $k[\mathcal{C}_1]$. Leveraging this criterion, we identify infinite families of projective curves satisfying this property.

INTRODUCTION

Let k be an infinite field, and $k[\mathbf{x}] := k[x_1, \dots, x_n]$ and $k[\mathbf{t}] := k[t_1, \dots, t_m]$ be two polynomial rings over k . Given $\mathcal{B} = \{b_1, \dots, b_n\} \subset \mathbb{N}^m$, a set of nonzero vectors, each element $b_i = (b_{i,1}, \dots, b_{i,m}) \in \mathbb{N}^m$ corresponds to the monomial $\mathbf{t}^{b_i} := t_1^{b_{i,1}} \dots t_m^{b_{i,m}} \in k[\mathbf{t}]$. The affine toric variety $X_{\mathcal{B}} \subset \mathbb{A}_k^n$ determined by $\mathcal{B}$ is the Zariski closure of the set given parametrically by $x_i = u_1^{b_{i,1}} \dots u_m^{b_{i,m}}$ for all $i = 1, \dots, n$. Consider

$$\mathcal{S}_{\mathcal{B}} := \langle b_1, \dots, b_n \rangle = \{\alpha_1 b_1 + \dots + \alpha_n b_n \mid \alpha_1, \dots, \alpha_n \in \mathbb{N}\} \subset \mathbb{N}^m,$$

the affine monoid spanned by $\mathcal{B}$. The toric ideal determined by $\mathcal{B}$ is the kernel $I_{\mathcal{B}}$ of the homomorphism of k -algebras $\varphi_{\mathcal{B}} : k[\mathbf{x}] \rightarrow k[\mathbf{t}]$ induced by $x_i \mapsto \mathbf{t}^{b_i}$. Since k is infinite, one has that $I_{\mathcal{B}}$ is the vanishing ideal of $X_{\mathcal{B}}$ and, hence, the coordinate ring of $X_{\mathcal{B}}$ is (isomorphic to) the monomial algebra $k[\mathcal{S}_{\mathcal{B}}] := \text{Im}(\varphi_{\mathcal{B}}) \simeq k[\mathbf{x}]/I_{\mathcal{B}}$. The ideal $I_{\mathcal{B}}$ is an $\mathcal{S}_{\mathcal{B}}$ -homogeneous binomial ideal, i.e., if one sets the $\mathcal{S}_{\mathcal{B}}$ -degree of a monomial $\mathbf{x}^{\alpha} \in k[\mathbf{x}]$ as $\deg_{\mathcal{S}_{\mathcal{B}}}(\mathbf{x}^{\alpha}) := \alpha_1 b_1 + \dots + \alpha_n b_n \in \mathcal{S}_{\mathcal{B}}$, then $I_{\mathcal{B}}$ is generated by $\mathcal{S}_{\mathcal{B}}$ -homogeneous binomials. One can thus consider a minimal $\mathcal{S}_{\mathcal{B}}$ -graded free resolution of $k[\mathcal{S}_{\mathcal{B}}]$ as $\mathcal{S}_{\mathcal{B}}$ -graded $k[\mathbf{x}]$ -module,

$$\mathcal{F} : 0 \rightarrow F_p \rightarrow \dots \rightarrow F_0 \rightarrow k[\mathcal{S}_{\mathcal{B}}] \rightarrow 0.$$

The projective dimension of $k[\mathcal{S}_{\mathcal{B}}]$ is $\text{pd}(k[\mathcal{S}_{\mathcal{B}}]) = \max\{i \mid F_i \neq 0\}$. The i -th Betti number of $k[\mathcal{S}_{\mathcal{B}}]$ is the rank of the free module F_i , i.e., $\beta_i(k[\mathcal{S}_{\mathcal{B}}]) = \text{rank}(F_i)$; and the Betti sequence of $k[\mathcal{S}_{\mathcal{B}}]$ is $(\beta_i(k[\mathcal{S}_{\mathcal{B}}])); 0 \leq i \leq \text{pd}(k[\mathcal{S}_{\mathcal{B}}])$. When the Krull dimension of $k[\mathcal{S}_{\mathcal{B}}]$

This work has been partially supported by the grant PID2022-137283NB-C22 funded by MCIN/AEI/10.13039/501100011033 and by ERDF “A way of making Europe”.

The third author thanks financial support from European Social Fund, *Programa Operativo de Castilla y León*, and *Consejería de Educación de la Junta de Castilla y León*.

The talk at the meeting EACA 2024 has been given by the third author.

coincides with its depth as $k[\mathbf{x}]$ -module, the ring $k[\mathcal{S}_B]$ is said to be Cohen-Macaulay. By the Auslander-Buchsbaum formula, this is equivalent to $\text{pd}(k[\mathcal{S}_B]) = n - \dim(k[\mathcal{S}_B])$. When $k[\mathcal{S}_B]$ is Cohen-Macaulay, its (Cohen-Macaulay) type is the rank of the last nonzero module in the resolution, i.e., $\text{type}(k[\mathcal{S}_B]) := \beta_p(k[\mathcal{S}_B])$ where $p = \text{pd}(k[\mathcal{S}_B])$.

Now consider $d \in \mathbb{Z}^+$ and $a_0 := 0 < a_1 < \dots < a_n = d$ a sequence of integers such that $\gcd(a_1, \dots, a_n) = 1$. Denote by $\mathcal{C}$ the projective monomial curve $\mathcal{C} \subset \mathbb{P}_k^n$ of degree d parametrically defined by $x_i = u^{a_i}v^{d-a_i}$ for all $i \in \{0, \dots, n\}$, i.e., $\mathcal{C}$ is the Zariski closure of

$$\{(u^{a_0}v^{d-a_0} : \dots : u^{a_i}v^{d-a_i} : \dots : u^{a_n}v^{d-a_n}) \in \mathbb{P}_k^n \mid (u : v) \in \mathbb{P}_k^1\}.$$

Taking $\mathcal{A} = \{\mathbf{a}_0, \dots, \mathbf{a}_n\} \subset \mathbb{N}^2$ with $\mathbf{a}_i = (a_i, d - a_i)$ for all $i = 0, \dots, n$, one has that $I_{\mathcal{A}}$ is the vanishing ideal of $\mathcal{C}$, and the coordinate ring of $\mathcal{C}$ is the two-dimensional ring $k[\mathcal{C}] = k[x_0, \dots, x_n]/I_{\mathcal{A}}$. The projective monomial curve $\mathcal{C}$ is said to be arithmetically Cohen-Macaulay if the ring $k[\mathcal{C}]$ is Cohen-Macaulay.

The projective curve $\mathcal{C}$ has two affine projections, $\mathcal{C}_1 = \{(u^{a_1}, \dots, u^{a_n}) \in \mathbb{A}_k^n \mid u \in k\}$ and $\mathcal{C}_2 = \{(v^{d-a_0}, v^{d-a_1}, \dots, v^{d-a_{n-1}}) \in \mathbb{A}_k^n \mid v \in k\}$, associated to the sequences $a_1 < \dots < a_n$ and $d - a_{n-1} < \dots < d - a_1 < d - a_0$, respectively. The second sequence is sometimes called the dual of the first one. Denote by $\mathcal{S}_1 := \mathcal{S}_{\mathcal{A}_1}$ the numerical semigroup generated by $\mathcal{A}_1 = \{a_1, \dots, a_n\}$. The vanishing ideal of $\mathcal{C}_1$ is $I_{\mathcal{A}_1} \subset k[x_1, \dots, x_n]$, and hence, its coordinate ring is the one-dimensional ring $k[\mathcal{C}_1] \simeq k[x_1, \dots, x_n]/I_{\mathcal{A}_1}$. Moreover, $I_{\mathcal{A}}$ is the homogenization of $I_{\mathcal{A}_1}$ with respect to the variable x_0 . Similarly, denoting by $\mathcal{S}_2 := \mathcal{S}_{\mathcal{A}_2}$ the numerical semigroup generated by $\mathcal{A}_2 = \{d - a_0, d - a_1, \dots, d - a_{n-1}\}$, the vanishing ideal of $\mathcal{C}_2$ is $I_{\mathcal{A}_2} \subset k[x_0, \dots, x_{n-1}]$, its coordinate ring is $k[\mathcal{C}_2] \simeq k[x_0, \dots, x_{n-1}]/I_{\mathcal{A}_2}$, and $I_{\mathcal{A}}$ is the homogenization of $I_{\mathcal{A}_2}$ with respect to x_n .

One has that $\beta_i(k[\mathcal{C}]) \geq \beta_i(k[\mathcal{C}_1])$ for all i , and the goal of this work is to understand when the Betti sequences of $k[\mathcal{C}]$ and $k[\mathcal{C}_1]$ coincide. A necessary condition is that $k[\mathcal{C}]$ is Cohen-Macaulay. Indeed, affine monomial curves are always arithmetically Cohen-Macaulay while projective ones may be arithmetically Cohen-Macaulay or not. Thus, $\text{pd}(k[\mathcal{C}]) = \text{pd}(k[\mathcal{C}_1])$ if and only if $\mathcal{C}$ is arithmetically Cohen-Macaulay. In Theorem 1.2, which is the main result of this work, we provide a combinatorial sufficient condition for having equality between the Betti sequences of $k[\mathcal{C}]$ and $k[\mathcal{C}_1]$ by means of the poset structures induced by $\mathcal{S}$ and $\mathcal{S}_1$ on the Apéry sets of both $\mathcal{S}$ and $\mathcal{S}_1$. In Propositions 2.1 and 2.3, we use our main result to provide explicit families of curves where $\beta_i(k[\mathcal{C}]) = \beta_i(k[\mathcal{C}_1])$ for all i .

The motivation of this work comes from [4], where the authors obtain a sufficient condition in terms of Gröbner bases to ensure the equality of the Betti sequences.

The computations in the examples given in this paper are performed using Singular [2].

1. APÉRY SETS AND BETTI NUMBERS

Let $d \in \mathbb{Z}^+$ and $a_0 := 0 < a_1 < \dots < a_n = d$ be a sequence of relatively prime integers. For each $i = 0, \dots, n$, set $\mathbf{a}_i := (a_i, d - a_i) \in \mathbb{N}^2$, and consider the three sets $\mathcal{A}_1 = \{a_1, \dots, a_n\}$, $\mathcal{A}_2 = \{d - a_1, \dots, d - a_{n-1}\}$ and $\mathcal{A} = \{\mathbf{a}_0, \dots, \mathbf{a}_n\} \subset \mathbb{N}^2$. We denote by $\mathcal{C} \subset \mathbb{P}_k^n$ the projective monomial curve defined by $\mathcal{A}$ as defined in the introduction, and by $\mathcal{C}_1$ and $\mathcal{C}_2$ its affine projections. Consider $\mathcal{S}_1$ and $\mathcal{S}_2$ the numerical semigroups generated

by $\mathcal{A}_1$ and $\mathcal{A}_2$ respectively, and $\mathcal{S}$ the monoid spanned by $\mathcal{A}$ that we call the homogenization of $\mathcal{S}_1$ (with respect to d).

Definition 1.1. For $i = 1, 2$, the Apery set of $\mathcal{S}_i$ with respect to d is $\text{Ap}_i := \{y \in \mathcal{S}_i \mid y - d \notin \mathcal{S}_i\}$. One can also define the Apery set of $\mathcal{S}$ as $\text{AP}_{\mathcal{S}} := \{\mathbf{y} \in \mathcal{S} \mid \mathbf{y} - \mathbf{a}_0 \notin \mathcal{S}, \mathbf{y} - \mathbf{a}_n \notin \mathcal{S}\}$.

Note that $\text{AP}_{\mathcal{S}}$ has at least d elements by [3, Lem. 2.5]. Moreover, $|\text{AP}_{\mathcal{S}}| = d$ if and only if $\mathcal{C}$ is arithmetically Cohen-Macaulay.

In order to compare $\beta_i(k[\mathcal{C}])$ and $\beta_i(k[\mathcal{C}_1])$ for all i , we will relate in Theorem 1.2 the Apery sets Ap_1 and $\text{AP}_{\mathcal{S}}$ with the natural poset structure that both have and that we now define. For $i = 1, 2$, $(\text{Ap}_i, \leq_i)$ is a poset, where $\leq_i$ is given by $y \leq_i z \iff z - y \in \mathcal{S}_i$. Similarly, $(\text{AP}_{\mathcal{S}}, \leq_{\mathcal{S}})$ is a poset for $\leq_{\mathcal{S}}$ defined by $\mathbf{y} \leq_{\mathcal{S}} \mathbf{z} \iff \mathbf{z} - \mathbf{y} \in \mathcal{S}$.

The main result in this section is Theorem 1.2 where we give a sufficient condition in terms of the poset structures of the Apery sets Ap_1 and $\text{AP}_{\mathcal{S}}$ for the Betti sequences of $k[\mathcal{C}_1]$ and $k[\mathcal{C}]$ to coincide.

Theorem 1.2. *If $(\text{AP}_{\mathcal{S}}, \leq_{\mathcal{S}}) \simeq (\text{Ap}_1, \leq_1)$, then $\beta_i(k[\mathcal{C}]) = \beta_i(k[\mathcal{C}_1])$ for all i .*

2. EXAMPLES OF APPLICATION

In Propositions 2.1 and 2.3, we provide some sequences $a_1 < \dots < a_n$ for which the condition in Theorem 1.2 is satisfied. Let us start with arithmetic sequences, i.e., sequences $a_1 < \dots < a_n$ such that $a_i = a_1 + (i - 1)e$ for some positive integer e . For this family, we refine [4, Cor. 4.2] that considers $a_1 > n - 1$.

Proposition 2.1. *Let $a_1 < \dots < a_n$ be an arithmetic sequence of relatively prime integers. Then, $(\text{AP}_{\mathcal{S}}, \leq_{\mathcal{S}}) \simeq (\text{Ap}_1, \leq_1)$ if and only if $a_1 > n - 2$. Therefore, if $a_1 > n - 2$, the Betti sequences of $k[\mathcal{C}_1]$ and $k[\mathcal{C}]$ coincide.*

Example 2.2. For the sequence $5 < 6 < 7 < 8 < 9 < 10$, one has that $a_1 = 5 > 4 = n - 2$. Therefore, the Apery sets $(\text{Ap}_1, \leq_1)$ and $(\text{AP}_{\mathcal{S}}, \leq_{\mathcal{S}})$ are isomorphic. Hence, by Theorem 1.2, the Betti sequences of $k[\mathcal{C}_1]$ and $k[\mathcal{C}]$ coincide. One can check that both are $(1, 11, 30, 35, 19, 4)$. The posets $(\text{Ap}_1, \leq_1)$ and $(\text{AP}_{\mathcal{S}}, \leq_{\mathcal{S}})$ in this example are shown in Figure 1.

In [1, Sect. 6], the authors studied the canonical projections of the projective monomial curve $\mathcal{C}$ defined by an arithmetic sequence $a_1 < \dots < a_n$ of relatively prime integers, i.e., the curve $\pi_r(\mathcal{C})$ obtained as the Zariski closure of the image of $\mathcal{C}$ under the r -th canonical projection $\pi_r : \mathbb{P}_k^n \dashrightarrow \mathbb{P}_k^{n-1}$, $(p_0 : \dots : p_n) \mapsto (p_0 : \dots : p_{r-1} : p_{r+1} : \dots : p_n)$. We know that $\pi_r(\mathcal{C})$ is the projective monomial curve associated to the sequence $a_1 < \dots < a_{r-1} < a_{r+1} < \dots < a_n$.

In Proposition 2.3, for any $r \in \{2, \dots, n - 1\}$, we consider $\mathcal{A}_1 = \{a_1, \dots, a_n\} \setminus \{a_r\}$, the numerical semigroup $\mathcal{S}_1 = \mathcal{S}_{\mathcal{A}_1}$, and its homogenization $\mathcal{S}$, and we characterize when the posets $(\text{Ap}_1, \leq_1)$ and $(\text{AP}_{\mathcal{S}}, \leq_{\mathcal{S}})$ are isomorphic.

Proposition 2.3. *Let $a_1 < \dots < a_n$ be an arithmetic sequence of relatively prime integers with $n \geq 4$, and $r \in \{2, \dots, n - 1\}$. Consider $\mathcal{A}_1 = \{a_1, \dots, a_n\} \setminus \{a_r\}$, the numerical*

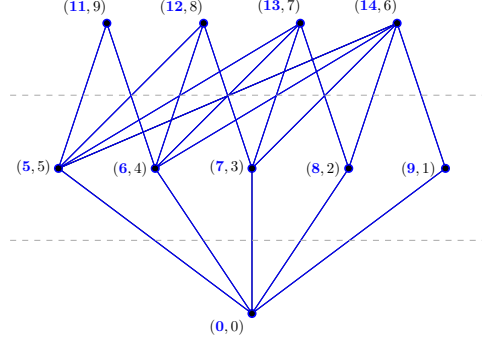


FIGURE 1. The posets $(\text{Ap}_1, \leq_1)$ (in blue) and $(\text{AP}_S, \leq_S)$ (in black) for $S_1 = \langle 5, 6, 7, 8, 9, 10 \rangle$.

semigroup S_1 generated by $\mathcal{A}_1$, and its homogenization S . Then the posets $(\text{Ap}_1, \leq_1)$ and $(\text{AP}_S, \leq_S)$ are isomorphic if and only if one of the following conditions holds:

- (a) $r = 2$, $a_1 \geq n - 1$ and $a_1 \neq n$;
- (b) $3 \leq r \leq n - 2$, $a_1 \geq n$ and $r \leq a_1 - n + 1$;
- (c) $r = n - 1$ and $a_1 \geq n - 2$.

Consequently, if one of the previous conditions holds, then $\beta_i(k[\mathcal{C}_1]) = \beta_i(k[\mathcal{C}])$, for all i .

Example 2.4. For the sequence $9 < 10 < 11 < 12 < 13$, the Betti sequences of $k[\mathcal{C}_1]$ and $k[\mathcal{C}]$ coincide by Proposition 2.1. Indeed, it is $(1, 10, 20, 15, 4)$ for both curves. The parameters of this arithmetic sequence are $a_1 = 9$, $e = 1$ and $n = 5$. Hence, the Betti sequences of $k[\pi_r(\mathcal{C}_1)]$ and $k[\pi_r(\mathcal{C})]$ coincide for $r = 2, 3, 4$ by Proposition 2.3. One can check that the Betti sequence of $k[\pi_2(\mathcal{C})]$ and $k[\pi_4(\mathcal{C})]$ is $(1, 5, 6, 2)$, and the Betti sequence of $k[\pi_3(\mathcal{C})]$ is $(1, 8, 12, 5)$.

REFERENCES

- [1] I. Bermejo, E. García-Llorente, I. García-Marco, and M. Morales. Noether resolutions in dimension 2. *J. Algebra* **482** (2017), 398-426.
- [2] W. Decker, G.-M. Greuel, G. Pfister, and H. Schönemann. Singular 4-3-0 — A computer algebra system for polynomial computations. <http://www.singular.uni-kl.de>, 2022.
- [3] P. Gimenez and M. González Sánchez. Castelnuovo-Mumford regularity of projective monomial curves via sumsets, *Mediterr. J. Math.* **20**, 287 (2023), 24 pp.
- [4] J. Saha, I. Sengupta, and P. Srivastava. Betti sequence of the projective closure of affine monomial curves. *J. Symb. Comput.* **119** (2023), 101-111.

Instituto de Matemáticas y Aplicaciones (IMAUULL), Sección de Matemáticas, Facultad de Ciencias, Universidad de La Laguna, 38200, La Laguna, Spain
Email address: iggarcia@ull.edu.es

Instituto de Investigación en Matemáticas de la Universidad de Valladolid (IMUVA), Universidad de Valladolid, 47011 Valladolid, Spain.
Email address: pgimenez@uva.es
Email address: mario.gonzalez.sanchez@uva.es

ON THE NUMBER OF TOEPLITZ FACTORS OF A MATRIX

IGNACIO GARCÍA-MARCO, IRENE MÁRQUEZ-CORBELLA, AND DANIEL SECO

ABSTRACT. In this work we consider factorizations of square complex matrices as product of Toeplitz matrices. We disprove a conjecture by Ye and Lim, by showing that there are 3×3 complex matrices which can't be expressed as the product of two Toeplitz matrices of the same size. We also improve existing upper bounds on the number of Toeplitz factors needed to express every $n \times n$ matrix with $n \leq 5$.

INTRODUCTION

Decomposing matrices as products of structured matrices has been proven to be a very effective technique in computational and numerical algebra and, for example, decompositions of matrices as the product of a lower-triangular and an upper-triangular matrix (LU), or of an orthogonal and an upper-triangular matrix (QR), or of two orthogonal matrices with a diagonal one (SVD), are ubiquitous in many numerical applications.

In this work, we study decompositions of square matrices as product of Toeplitz matrices. A square $n \times n$ complex matrix $T = (a_{i,j}) \in \mathcal{M}_{n \times n}(\mathbb{C})$ is *Toeplitz* if its entries are constant along the diagonals, i.e.,

$$T = \begin{pmatrix} t_0 & t_1 & & t_{n-1} \\ t_{-1} & t_0 & \ddots & \\ & \ddots & \ddots & t_1 \\ t_{-(n-1)} & & t_{-1} & t_0 \end{pmatrix},$$

or, in other words, there exists $\{t_k \mid -(n-1) \leq k \leq n-1\} \subset \mathbb{C}$ such that $a_{i,j} = t_{j-i}$ for all $i, j \in \{1, \dots, n\}$. Toeplitz matrices are one of the most well-studied and understood classes of structured matrices and present several interesting computational advantages. For example, linear systems involving Toeplitz matrices can be solved in $\mathcal{O}(n \log^2(n))$ operations (see [1]).

Given a square matrix $A \in \mathcal{M}_{n \times n}(\mathbb{C})$, Ye and Lim proved in [3] that A can be written as

$$A = T_1 \cdots T_s,$$

where $T_1, \dots, T_s$ are Toeplitz $n \times n$ matrices. Any such writing of a matrix will be called a *Toeplitz decomposition of length s* . These decompositions have many attractive computational properties and are precious in computational algebra, for example if one knows a Toeplitz decomposition of length s of a matrix A , then one can solve linear systems in A

The first and second authors have been partially supported by the Spanish grant MICINN PID2019-105896GB-I00.

The talk at the meeting EACA 2024 has been given by the first author.

within $\mathcal{O}(sn(\log^2(n)))$ operations. The minimum length among all the Toeplitz decompositions of a matrix will be called the *Toeplitz rank* of the matrix A and will be denoted by $\text{TR}(A)$. In [3, Theorem 3.1, Corollary 5.3 and Theorem 5.5] the authors prove the following:

Theorem 0.1. *Let $A \in \mathcal{M}_{n \times n}(\mathbb{C})$, then*

- (a) $\text{TR}(A) \leq \lfloor n/2 \rfloor + 1$ if A is generic (in the Zariski topology sense),
- (b) $\text{TR}(A) \leq n + 2$, if A is invertible, and
- (c) $\text{TR}(A) \leq 2n + 5$.

By a dimension counting argument they derive that the bound in Theorem 0.1.(a) is sharp, and they wonder if (b) and (c) can be improved. More precisely, they conjecture that the generic bound works for all the matrices:

Conjecture 0.2. [3, Conjecture 5.6] *Every matrix $A \in \mathcal{M}_{n \times n}(\mathbb{C})$ is a product of at most $\lfloor n/2 \rfloor + 1$ Toeplitz matrices.*

If one defines $\text{TR}_{\max}(n)$ as the maximum Toeplitz rank among all the $n \times n$ matrices, Ye and Lim's results imply that

$$(1) \quad \lfloor n/2 \rfloor + 1 \leq \text{TR}_{\max}(n) \leq 2n + 5;$$

and the conjecture is equivalent to $\text{TR}_{\max}(n) = \lfloor n/2 \rfloor + 1$.

The goal of this work is to study the values of $\text{TR}_{\max}(n)$ for small values of n .

1. COUNTEREXAMPLES TO THE CONJECTURE IN $n = 3$

A simple and key observation is that given an $n \times n$ matrix A and a value $s \in \mathbb{Z}^+$, determining whether A admits a Toeplitz decomposition of length s is equivalent to the problem of deciding if a particular system of multivariate polynomial equations has complex solutions. More precisely:

Proposition 1.1. *Let $A = (a_{i,j}) \in \mathcal{M}_{n \times n}(\mathbb{C})$ be an $n \times n$ matrix and $s \geq 1$. Consider the set of $(2n - 1)s$ variables $X = \{x_{k,\ell} \mid 1 \leq k \leq s, -(n - 1) \leq \ell \leq n - 1\}$, and the n^2 homogeneous polynomials of degree s*

$$f_{i,j} := \sum_{1 \leq l_1, \dots, l_{s-1} \leq n} x_{1,l_1-i} x_{2,l_2-l_1} \cdots x_{s,j-l_{s-1}} \in \mathbb{C}[X], \text{ for } i, j \in \{1, \dots, n\}.$$

The following conditions are equivalent:

- *The matrix $A \in \mathcal{M}_{n \times n}(\mathbb{C})$ is a product of s Toeplitz matrices.*
- *The system of equations $f_{i,j} = a_{i,j}$ for all $i, j \in \{1, \dots, n\}$ has a solution in $\mathbb{C}^{(2n-1)s}$.*
- *The ideal $I = \langle f_{i,j} - a_{i,j} \mid 1 \leq i, j \leq n \rangle \subseteq \mathbb{C}[X]$ satisfies that $1 \notin I$.*

This result might suggest Gröbner basis techniques to compute Toeplitz ranks of matrices. However, due to the size of the problem, this approach seems to be useless even for quite small values of n and s ($n \geq 4$ and $s \geq 3$). Nevertheless, as the following example shows, for $n = 3$ one can effectively check if a certain matrix has a Toeplitz decomposition of length 2.

Example 1.2. Consider the 3×3 diagonal matrix

$$A = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}.$$

The following extract from SAGEMATH [2] shows that the ideal I described in Proposition 1.1 is $I = \langle 1 \rangle$ and, hence, A cannot be written as a product of two Toeplitz matrices.

```
In: R.<a0,a1,a2,a3,a4,b0,b1,b2,b3,b4>=PolynomialRing(QQ,10,order='deglex');
    A=matrix(R,[[a2,a3,a4],[a1,a2,a3],[a0,a1,a2]])
    B=matrix(R,[[b2,b3,b4],[b1,b2,b3],[b0,b1,b2]])
    M=matrix(R,[[0,0,0],[0,1,0],[0,0,2]])
    S=A*B-M
    I= R.ideal([S[i][j] for i in range(3) for j in range(3)])
    G=I.groebner_basis()
    G
Out: [1]
```

Thus, A is a counterexample to Conjecture 0.2 and we have that $\text{TR}_{\max}(3) \geq 3$.

In fact, one can extend this example and prove that most diagonal 3×3 matrices cannot be expressed as a product of 2 Toeplitz matrices; providing an infinite family of counterexamples to Conjecture 0.2.

Proposition 1.3. *Let $d_1, d_2, d_3 \in \mathbb{C}$ and consider the matrix*

$$A = \begin{pmatrix} d_1 & 0 & 0 \\ 0 & d_2 & 0 \\ 0 & 0 & d_3 \end{pmatrix},$$

$$\text{then } \text{TR}(A) = \begin{cases} 2 & \text{if } (d_1 - d_2)(d_1 - d_3)(d_2 - d_3)d_2 = 0, \text{ or} \\ 3 & \text{otherwise} \end{cases}$$

We have produced further counterexamples to Conjecture 0.2 as, for example, the anti-symmetric matrix

$$A = \begin{pmatrix} 0 & 1 & 2 \\ -1 & 0 & 4 \\ -2 & -4 & 0 \end{pmatrix},$$

which satisfies that $\text{TR}(A) = 3$.

We have not been able to produce counterexamples for the conjecture for $n \geq 4$. In this setting we have verified that most diagonal 4×4 matrices (those whose diagonal entries d_1, d_2, d_3, d_4 are nonzero, different and do not satisfy that $d_1 d_4 = d_2 d_3$) admit a Toeplitz decomposition of length 3.

2. MAXIMUM TOEPLITZ RANK OF SMALL SIZE MATRICES

For low rank matrices one can devise explicit algorithms for finding Toeplitz decompositions

Proposition 2.1. *Let $A \in \mathcal{M}_{n \times n}(\mathbb{C})$ be a matrix of rank at most 2, then $\text{TR}(A) \leq 4$.*

Also for $n \times n$ matrices of rank $n - 1$, one has the following.

Proposition 2.2. *Let $A \in \mathcal{M}_{n \times n}(\mathbb{C})$ of rank $n - 1$, then $A = PT_1 T_2$, with P an invertible matrix and T_1, T_2 two Toeplitz matrices.*

From these propositions, together with Ye-Lim's results, Proposition 1.3 and a careful inspection of 5×5 matrices of rank 3, we get the following improvement of the bounds in (1) for $\text{TR}_{\max}(n)$ and $n \in \{3, 4, 5\}$.

Theorem 2.3. *Let $\text{TR}_{\max}(n)$ be the maximum Toeplitz rank of an $n \times n$ matrix, then:*

- $3 \leq \text{TR}_{\max}(3) \leq 4$,
- $3 \leq \text{TR}_{\max}(4) \leq 8$, and
- $3 \leq \text{TR}_{\max}(5) \leq 10$.

REFERENCES

- [1] R.B. Bitmead, B.D.O. Anderson, Asymptotically fast solution of Toeplitz and related systems of linear equations, *Linear Algebra Appl.*, 34 (1980), pp. 103–116.
- [2] SageMath, the Sage Mathematics Software System (Version 10.2), The Sage Developers, 2024, <https://www.sagemath.org>.
- [3] K. Ye, L.-H. Lim, Every Matrix is a Product of Toeplitz Matrices. *Found. Comput. Math.* 16(3): 577-598 (2016).

Instituto de Matemáticas y Aplicaciones (IMAUULL), Sección de Matemáticas, Facultad de Ciencias, Universidad de La Laguna, 38200, La Laguna, Spain

Email address: `iggarcia@ull.edu.es`

Email address: `imarquec@ull.edu.es`

Email address: `dsecofor@ull.edu.es`

HADAMARD QUASIGROUP PRODUCTS PRESERVING THE LATIN SQUARE CONDITION

MANUEL GONZÁLEZ-REGADERA, MARÍA DOLORES FRAU, AND RAÚL M. FALCÓN

ABSTRACT. The Hadamard quasigroup product has recently been introduced as a natural generalization of the classical Hadamard product of matrices. It constitutes a superposition operator of three binary operations, one of them being a quasigroup operation. In this paper, we make use of a computational algebraic geometry approach to deal with the set of Latin squares whose successive powers according to the Hadamard quasigroup product is again a Latin square. The performed computation ensures the existence of Latin squares for which the smallest power before recovering the initial Latin square is greater than its order.

INTRODUCTION

Let $\mathcal{A}(n)$ be the set of $n \times n$ arrays with entries in the set of symbols $[n] := \{1, \dots, n\}$. Every binary operation f on the set $[n]$ is uniquely identified by its multiplication table $A_f \in \mathcal{A}(n)$ so that $A_f[i, j] := f(i, j)$ for all $i, j \in [n]$. A binary operation is a *superposition* if it results after permuting, identifying or adding variables in an operation, or replacing variables by operations [4]. This paper focuses on the superposition operator associated to three binary operations f, g and h as follows.

$$\begin{aligned} \odot_f(g, h) : [n] \times [n] &\longrightarrow [n] \\ (i, j) &\mapsto f(g(i, j), h(i, j)) \end{aligned}$$

Equivalently, $\odot_{A_f}(A_g, A_h)[i, j] := A_f[A_g[i, j], A_h[i, j]]$ for all $i, j \in [n]$. More specifically, we are interested in the case in which A_f describes a *Latin square*. That is, an array $L \in \mathcal{A}(n)$ such that each symbol in the set $[n]$ appears exactly once per row, and exactly once per column. From now on, we denote by $\mathcal{L}(n)$ the set of such arrays. Every Latin square $L \in \mathcal{L}(n)$ constitutes the multiplication table of a *quasigroup* $([n], *)$ of order n . That is, the set $[n]$ is endowed with a binary operation $*$, so that both equations $i * x = j$ and $y * i = j$ have unique solutions $x, y \in [n]$, for all $i, j \in [n]$. The superposition operator $\odot_L(A, B)$, with $L \in \mathcal{L}(n)$ and $A, B \in \mathcal{A}(n)$ is called a *Hadamard quasigroup product*, which has recently been introduced [1] as a natural generalization of the classical Hadamard product. If $A = B = L$, then, for every positive integer $k \geq 2$, it is also defined the product

$$(1) \quad \odot_\rho^k L := \odot_L \left(\odot_\rho^{k-1} L, L \right)$$

The first author thanks the Institute of Mathematics of the University of Seville (IMUS) for its Program PI3 for Introduction to Research, under which this work was started. This work is partially supported by the research project TED2021-130566B-I00 “*New graphical authentication schemes in Information Management Systems by means of fractal images based on Latin squares*” from the Ministry of Science and Innovation of the Government of Spain, and also by the PAIDI research group FQM-016 from Junta de Andalucía.

The talk at the meeting EACA 2024 has been given by Manuel González-Regadera.

where $\odot_\rho^1 L := L$. The discrete structure of the Latin square L endows this product with a cyclic behaviour, so that one can ensure the existence of a positive integer k such that $\odot_\rho^{k+1} L = L$. The minimum positive integer $\rho(L)$ satisfying this condition is a Latin square isomorphism invariant [1]. Of particular interest, it is defined the set $\mathcal{HL}_\rho(n) := \{L \in \mathcal{L}(n) : \odot_\rho^k L \in \mathcal{L}(n) \text{ for all } k \leq \rho(L)\}$. An algebraic geometry approach was described in [1] to classify up to isomorphism all the Latin squares $L \in \mathcal{HL}_\rho(n)$, for all $n \leq 6$. All of them satisfy that $\rho(L) \leq n$, and also that the permutations defined by each column in L have the same cycle structure. We prove that these conditions are not satisfied in general. To this end, we make use of an alternative computational algebraic geometry approach, which enables us to deal with higher orders.

1. OUR COMPUTATIONAL ALGEBRAIC GEOMETRY APPROACH

Every array $A \in \mathcal{A}(n)$ is uniquely determined by its set of entries $\text{Ent}(A) := \{(i, j, A[i, j]) : i, j \in [n]\}$. Let S_n be the symmetric group on the set $[n]$. A *Latin transversal* in A is any subset $T \subseteq \text{Ent}(A)$ containing exactly one entry per row, exactly one entry per column, and exactly one entry per symbol. It describes a permutation $\pi_T \in S_n$ so that $\pi_T(j) := A[i_j, j]$, with $(i_j, j) \in T$. The following result shows how Latin squares in $\mathcal{HL}_\rho(n)$ require the existence of successive localized Latin transversals in L .

Proposition 1.1 ([1]). *If $L \in \mathcal{L}(n)$, then the following statements hold.*

- a) $L \in \mathcal{HL}_\rho(n)$ if and only if the subset of entries
- $$(2) \quad T_k(L) := \left\{ \left(\odot_\rho^k L[i, i], L[i, i], \odot_\rho^{k+1} L[i, i] \right) : i \in [n] \right\} \subseteq \text{Ent}(L)$$
- is a Latin transversal for every positive integer k . Moreover, $T_k(L) = T_{k+l\rho(L)+1}(L)$ for every pair of positive integers k, l .*
 - b) *In particular, $L^2 \in \mathcal{L}(n)$ if and only if the main diagonal $T_1(L)$ is a Latin transversal.*
 - c) *Let $\pi_1, \pi_2 \in S_n$ be two permutations with the same cycle structure. Then, there is a one-to-one correspondence from the subset of Latin squares $L' \in \mathcal{HL}_\rho(n)$ such that $\pi_{T_1(L')} = \pi_1$ to that of Latin squares $L'' \in \mathcal{HL}_\rho(n)$ such that $\pi_{T_1(L'')} = \pi_2$.*

The union of entries of all the Latin transversals defined in (2) describes uniquely a *partial Latin square* of order n . That is, an $n \times n$ array with symbols in the set $[n]$ such that every symbol appears at most once per row, and at most once per column. Every Latin square to which this partial Latin square can be completed belongs to $\mathcal{HL}_\rho(n)$. This last set can be determined from a sequential construction of feasible Latin transversals defined as in (2), for which the union of their respective entries respects the Latin square condition. The third statement of Proposition 1.1 enables one to start this construction with representative main diagonals describing permutations with distinct cycle structures. A computational algebraic geometry approach based on the ideas described in [2] was proposed in [1] to determine this sequential construction (and hence, the set $\mathcal{HL}_\rho(n)$) for all $n \leq 6$. (The case $n = 7$ was not possible to be determined due the computational complexity of the method therein described.) To deal with higher orders, we propose here an alternative computational algebraic geometry approach based on the ideas described in [3]. To this end, let T_1 be the main diagonal from which the sequence under construction starts. In addition, let $T_2, \dots, T_k$ be subsequent feasible Latin transversals that are already known in

that sequence. (If $k = 1$, then we only know T_1 .) Based on the first statement of Proposition 1.1, we assume here that $T_i \neq T_1$ for all $i \leq k$. Then, let P_k be the partial Latin square satisfying that $\text{Ent}(P_k) = \bigcup_{i=1}^k \text{Ent}(T_i)$. To compute the set of subsequent feasible Latin transversals T_{k+1} , let $\mathbb{Q}[X_n]$ be the multivariate polynomial ring over the field of rational numbers, with $X_n := \{x_{ij} : i, j \in [n]\}$. Then, the sought set is identified with the algebraic set $\mathcal{V}(I_{P_k})$ of the zero-dimensional ideal $I_{P_k} := \langle x_{ij} \cdot (x_{ij} - 1), \sum_{j=1}^n x_{ij} - 1, x_{ij}x_{i'j} : i, j, i' \in [n], i \neq i' \rangle \cup \langle x_{ij} : i, j \in [n], P_k[\pi_{T_k}(i), i] \in [n] \rangle \cup \langle x_{iP_k[j,i]} : i, j \in [n], P_k[j, i] \in [n] \rangle \cup \langle x_{iP_k[\pi_{T_k}(i), j]} : i, j \in [n], P_k[\pi_{T_k}(i), j] \in [n] \rangle$ in the multivariate polynomial ring $\mathbb{Q}[X_n]$. The computation of the reduced Gröbner basis of this ideal make easier to determine this algebraic set. This procedure is iterated for each feasible Latin transversal $T_{k+1} \in \mathcal{V}(I_{P_k})$ such that $T_{k+1} \neq T_1$. The iteration finishes once we recover the initial Latin transversal T_1 in each sequence. (It always occurs due to the first statement of Proposition 1.1 and the finite number of Latin squares of a given order.)

At this point, each obtained sequence $T_1, \dots, T_\rho$ determines a unique partial Latin square P_ρ , whose completions are Latin squares in the set $\mathcal{HL}_\rho(n)$. Each completion can sequentially be constructed by following an analogous computational algebraic geometry approach, but column-by-column instead that Latin transversal by Latin transversal. Note here that every column j in a Latin square $L \in \mathcal{HL}_\rho(n)$ describes a unique permutation $\pi_{L,j}^{\text{col}} \in S_n$ such that $\pi_{L,j}^{\text{col}}(i) = L[i, j]$ for all $i \in [n]$. Thus, columns play exactly the same role in the new procedure that Latin transversals do in the previous one. Of particular interest, we highlight each cycle $C_{L,j}$, with $j \in [n]$, containing the symbol j in the unique decomposition of the permutation $\pi_{L,j}^{\text{col}}$ into disjoint cycles. The relevance of these cycles is shown in the next result, which follows readily from the Hadamard quasigroup product described in (1).

Lemma 1.2. *Let $L \in \mathcal{HL}_\rho(n)$. Then, $\rho(L) = \text{lcm}\{|C_{L,j}| : j \in [n]\}$.*

For each Latin square $L \in \mathcal{HL}_\rho(n)$, let us consider the expression $z_L := n^{d_n^L} \dots 1^{d_1^L}$, where, for each $l \in [n]$, we denote by d_l^L the number of cycles of length l in the set $\{C_{L,1}, \dots, C_{L,n}\}$. For $n \leq 6$, the following two conditions hold (see [1]):

- (C.1) If $L \in \mathcal{HL}_\rho(n)$, then $d_i \cdot d_j = 0$ whenever $1 < i < j \leq n$. Hence, the corresponding parameter $\rho(L)$ is uniquely determined by any non-trivial cycle $C_{L,j}$.
- (C.2) $\rho(L) \leq n$ for all $n \leq 6$.

Of course, (C.1) implies (C.2). A main motivation to develop the current work is to know whether these two conditions holds for every order n . Determining the set $\mathcal{HL}_\rho(n)$ for small orders $n > 6$ can help in this regard.

2. COMPUTING HADAMARD QUASIGROUP PRODUCTS

We have implemented the previous procedures in the open computer algebra system for polynomial computations SINGULAR, available from <http://www.singular.uni-kl.de>. They have been used to determine the set $\mathcal{HL}_\rho(n)$ for distinct small values $n > 6$. As an illustrative example, we show here a representative Latin square L for each feasible expression z_L , where $L \in \mathcal{HL}_\rho(7)$ is a Latin square whose main diagonal describes a permutation of the longest possible length. The maximum running time that is required to compute any of them has been less than 10^{-4} seconds in an *Intel Core i7-8750H CPU (6 cores)*, with a *2.2 GHz processor and 8 GB of RAM*.

2	6	1	3	4	5	7
1	3	5	7	2	4	6
5	2	4	6	7	1	3
6	7	3	5	1	2	4
7	1	2	4	6	3	5
3	4	6	1	5	7	2
4	5	7	2	3	6	1

$$z_L = 2^7 \Rightarrow \rho(L) = 2$$

2	6	3	7	4	1	5
6	3	7	4	1	5	2
3	7	4	1	5	2	6
7	4	1	5	2	6	3
4	1	5	2	6	3	7
1	5	2	6	3	7	4
5	2	6	3	7	4	1

$$z_L = 3^7 \Rightarrow \rho(L) = 3$$

2	7	3	6	1	5	4
5	3	1	4	7	2	6
7	6	4	2	5	1	3
4	1	7	5	3	6	2
3	5	2	1	6	4	7
1	4	6	3	2	7	5
6	2	5	7	4	3	1

$$z_L = 4^7 \Rightarrow \rho(L) = 4$$

2	4	7	3	1	6	5
6	3	5	1	4	2	7
1	7	4	6	2	5	3
4	2	1	5	7	3	6
7	5	3	2	6	1	4
5	1	6	4	3	7	2
3	6	2	7	5	4	1

$$z_L = 6^7 \Rightarrow \rho(L) = 6$$

2	6	1	4	3	5	7
4	3	2	7	5	1	6
7	5	4	3	1	6	2
1	7	6	5	4	2	3
3	2	7	1	6	4	5
5	1	3	6	2	7	4
6	4	5	2	7	3	1

$$z_L = 3^6 2 \Rightarrow \rho(L) = 6$$

The last array does not satisfies Condition (C.1), so this condition does not hold in general. Furthermore, the following array was obtained so that it does not satisfy either of the two conditions (C.1) and (C.2).

2	5	12	4	8	7	13	14	15	16	3	6	10	11	1	9
3	1	7	8	11	6	14	15	5	13	16	2	9	12	10	4
4	6	5	2	10	15	7	13	11	8	14	3	16	1	9	12
5	15	9	3	14	1	6	8	2	4	7	13	11	16	12	10
1	3	8	9	6	16	11	4	13	12	15	14	5	10	7	2
10	2	11	12	7	4	3	5	14	15	9	16	1	13	8	6
9	12	3	10	1	2	8	6	16	14	13	15	4	5	11	7
15	14	2	1	5	13	4	7	3	6	8	10	12	9	16	11
13	7	14	15	16	3	5	9	10	11	6	12	2	8	4	1
14	10	15	7	13	5	16	2	12	9	11	1	8	4	6	3
16	13	4	5	15	14	1	11	7	10	12	9	3	6	2	8
12	4	16	13	3	8	15	1	9	7	10	11	6	2	14	5
6	8	10	11	9	12	2	16	1	5	4	7	14	3	15	13
7	9	6	16	12	11	10	3	8	1	2	4	13	15	5	14
11	16	1	6	2	9	12	10	4	3	5	8	7	14	13	15
8	11	13	14	4	10	9	12	6	2	1	5	15	7	3	16

$$z_L = 5^8 3^4 2^3 1 \Rightarrow \rho(L) = 30$$

REFERENCES

- [1] Falcón R.M., Álvarez V. Armario J.A., Frau M.D., Gudiel F., Güemes M.B. (2023): *A computational approach to analyze the Hadamard quasigroup product*. Electron. Res. Arch. **31**, 3245–3263, doi: 10.3934/era.2023164.
- [2] Falcón R.M., Martín-Morales J. (2007): *Gröbner bases and the number of Latin squares related to autotopisms of order ≤ 7* . J. Symb. Comput. **42**, 1142–1154, doi: 10.1016/j.jsc.2007.07.004.
- [3] Falcón R.M., Stones R.J. (2020): *Enumerating partial Latin rectangles*. Electron. J. Comb. **27**, paper P2.47, doi: 10.37236/9093
- [4] Lau D. (2006): *Function algebras on finite sets*, Springer Berlin, Heidelberg.

Universidad de Sevilla

Email address: manuelgonzalezregadera@gmail.com

Universidad de Sevilla

Email address: mdfrau@us.es

Universidad de Sevilla

Email address: rafalgan@us.es

A COMBINATORIAL APPROACH TO MODULI SPACES OF LINE ARRANGEMENTS

BENOÎT GUERVILLE-BALLÉ AND JUAN VIU-SOS

ABSTRACT. The *moduli space* $\mathcal{M}(\mathcal{A})$ of a line arrangement $\mathcal{A}$ in $\mathbb{CP}^2$ is the space of arrangements with the same combinatorial information as $\mathcal{A}$ (i.e. incidence relations between lines) up to linear projective transformations.

In a recent paper [GBVS23], we present some combinatorial techniques in order to determine topological and geometrical information of $\mathcal{M}(\mathcal{A})$ using combinatorial classes of arrangements characterized by a recursive structure, after the seminal work by Nazir and Yoshinaga in 2011. In particular, combinatorial methods to obtain a sharpened upper bound of connected components of $\mathcal{M}(\mathcal{A})$ are implemented.

INTRODUCTION

Complex projective line arrangements are fundamental objects in algebraic geometry, algebraic topology, and also combinatorics. The moduli space of a line arrangement $\mathcal{A}$ is a geometrical object which describes isomorphism classes (under the natural action of $\mathrm{PGL}_3(\mathbb{C})$) of arrangements that are lattice-isomorphic to $\mathcal{A}$. The topological study of the moduli space is extremely important in this context, e.g. arrangements in the same connected component of the moduli space have diffeomorphic complements [Ran89].

In a recent paper [GBVS23], we focus on a combinatorial study of the moduli space of line arrangements and we explore how such a study can provide fundamental information about its geometry and topology, introducing a combinatorial upper bound on the number of connected components of the moduli space of an arrangement.

We first define the notion of *m-perturbation* which transforms any combinatorics into an inductively connected one (Definition 2.2). By the work of Nazir and Yoshinaga [NY12], this allows to embed the moduli space of our original arrangement in an affine space of a relatively small dimension [GBVS23, Thm. 4.5]. From this embedding, we present in Section 2 an algorithm to compute an upper bound of the number of connected components of the moduli space by inductively bounding the degree of m polynomial conditions arising from a m -perturbation. Finally, in Section 3 we provide an example of family of arrangements where this upper bound is computed, showing that it is sharp when the number of connected components is arbitrarily large.

All the previous methods would be implemented in **Sagemath** [Sage].

The first author was partially supported by RIMS and JSPS KAKENHI Grant JP23H00081 (PI: Masahiko Yoshinaga).

The second author was partially supported by the Spanish grants PID2020-114750GB-C32/AEI/10.13039/501100011033 and MTM2016-76868-C2-2-P.

The talk at the meeting EACA 2024 has been given by the second author.

1. MODULI SPACES

Let Arr_n be the class of arrangements of n lines, for $n \geq 1$.

Definition 1.1. An *abstract line combinatorics* is a pair $\mathcal{C} = (\mathcal{L}, \mathcal{P})$ where:

- $\mathcal{L}$ is the data of an ordered set of n lines, codified by the list $\mathcal{L} = \{1, \dots, n\}$,
- $\mathcal{P}$ is a finite subset of the power set of $\mathcal{L}$ codifying the *singular points*, satisfying:
 - (1) for all $P \in \mathcal{P}$, one has $|P| \geq 2$,
 - (2) for all $i, j \in \mathcal{L}$, there exists a unique $P \in \mathcal{P}$ such that $i, j \in P$.

Two abstract line combinatorics $\mathcal{C} = (\mathcal{L}, \mathcal{P})$ and $\mathcal{C}' = (\mathcal{L}', \mathcal{P}')$ are called *equivalent*, denoted $\mathcal{C} \simeq \mathcal{C}'$, if there exists a (non-necessarily order-preserving) bijection $\Phi : \mathcal{L} \rightarrow \mathcal{L}'$ such that $\Phi(\mathcal{P}) = \mathcal{P}'$.

Any $\mathcal{A} \in \text{Arr}_n$ defines an abstract line combinatorics $\mathcal{C}(\mathcal{A}) = (\mathcal{A}, \mathcal{P}_{\mathcal{A}})$ in a natural way, where $\mathcal{P}_{\mathcal{A}}$ is derived from the bijection between the singular points of $\mathcal{A}$ and the lines meeting at these points. A *multiple point* of $\mathcal{C}(\mathcal{A})$ is an element $P \in \mathcal{P}_{\mathcal{A}}$ such that $|P| \geq 3$.

Definition 1.2. Let $\mathcal{C} = (\mathcal{L}, \mathcal{P})$ be an abstract line combinatorics, and let n be the cardinality of $\mathcal{L}$. The *moduli space* of $\mathcal{C}$ is the set:

$$\mathcal{M}(\mathcal{C}) = \{\mathcal{B} \in \text{Arr}_n \mid \mathcal{C}(\mathcal{B}) \simeq \mathcal{C}\} / \text{PGL}_3(\mathbb{C}).$$

For brevity sake, we set $\mathcal{M}(\mathcal{A}) := \mathcal{M}(\mathcal{C}(\mathcal{A}))$ for any $\mathcal{A} \in \text{Arr}_n$ with combinatorics $\mathcal{C}(\mathcal{A})$.

An *ordered arrangement* is a pair $(\mathcal{A}, \omega)$, where $\mathcal{A} \in \text{Arr}_n$ and ω is a bijective map

$$\omega : \mathcal{A} \longrightarrow \{1, \dots, n\},$$

called the *order* on $\mathcal{A}$. Let $\mathcal{A}_i = \omega^{-1}(\{1, \dots, i\})$, for $i \in \{1, \dots, n\}$. When ω is the order given by the indices, then $\mathcal{A}_i = \{\ell_1, \dots, \ell_i\}$. Consider the following ascending chain of (ordered) arrangements:

$$(1) \quad \mathcal{A}_1 = \{\ell_1\} \subsetneq \mathcal{A}_2 \subsetneq \dots \subsetneq \mathcal{A}_i \subsetneq \dots \subsetneq \mathcal{A}_n = \mathcal{A},$$

We denote by $\tau_i(\mathcal{A}, \omega)$ (alternatively, τ_i depending on the context) the cardinality of the intersection $|\omega^{-1}(i) \cap \text{Sing}(\mathcal{A}_{i-1})|$. Roughly speaking, τ_i counts the number of multiple points of $\mathcal{A}_i$ contained in the i th line.

Definition 1.3. The *type* of an ordered arrangement $(\mathcal{A}, \omega)$ is $\tau(\mathcal{A}, \omega) = (\tau_1, \dots, \tau_n) \in \mathbb{N}^n$.

Both the ascending chain (1) and the type can be defined for an abstract line combinatorics $\mathcal{C}$: by abuse of notation, we will also denote $(\mathcal{C})_1 \subsetneq \dots \subsetneq (\mathcal{C})_n = \mathcal{C}$ and $\tau(\mathcal{C}, \omega)$.

Definition 1.4 ([NY12, Def. 3.4]). An arrangement $\mathcal{A}$ is *inductively connected* if there exists an order ω on $\mathcal{A}$ such that $\max(\tau(\mathcal{A}, \omega)) \leq 2$.

Proposition 1.5 ([GBVS23, Propo. 3.4]). *If $\mathcal{A}$ is an inductively connected arrangement such that $\mathcal{A}$ is neither a pencil or a near-pencil¹, then $\mathcal{M}(\mathcal{A})$ is isomorphic to a Zariski open subset of a complex space of dimension $\dim_{\mathbb{C}} \mathcal{M}(\mathcal{A}) = \sum_{i=5}^n (2 - \tau_i)$. As a consequence, the moduli space $\mathcal{M}(\mathcal{A})$ is connected.*

¹An arrangement $\mathcal{A}$ is a *pencil* (resp. *near-pencil*) if $\mathcal{A}$ has at most one singular point (resp. if $\mathcal{A}$ is a pencil together with a generic line).

2. A COMBINATORIAL UPPER BOUND FOR THE NUMBER OF CONNECTED COMPONENTS

In this section, we present an algorithm that provides the formula for the upper bound on the number of connected components $\#\text{CC}(\mathcal{M}(\mathcal{A}))$ of a moduli space $\mathcal{M}(\mathcal{A})$.

Definition 2.1. Let $\mathcal{C} = (\mathcal{L}, \mathcal{P})$ be an abstract line combinatorics. Let $P_0 \in \mathcal{P}$ be a fixed multiple point of $\mathcal{C}$ and let $\ell \in P_0$. An *elementary perturbation* of $\mathcal{C}$ at (ℓ, P_0) is an abstract combinatorics $\tilde{\mathcal{C}} = (\mathcal{L}, \tilde{\mathcal{P}})$ such that:

- (1) for all $P \in \mathcal{P}$, $P \neq P_0$, one has $P \in \tilde{\mathcal{P}}$,
- (2) $\tilde{P}_0 = P_0 \setminus \{\ell\}$ is in $\tilde{\mathcal{P}}$.

Such a relation is denoted $\tilde{\mathcal{C}} \prec \mathcal{C}$. For any multiple point $P \in \mathcal{P}$, we call the *parent* of P in $\tilde{\mathcal{C}}$ the unique element $\tilde{P} \in \tilde{\mathcal{P}}$ such that either $\tilde{P} = P$ or $\tilde{P} = \tilde{P}_0$.

Definition 2.2. A *m-perturbation* of $\mathcal{C} = (\mathcal{L}, \mathcal{P})$ is a sequence of m elementary perturbations such that

$$\mathcal{C}_0 \prec \mathcal{C}_1 \prec \cdots \prec \mathcal{C}_m = \mathcal{C}, \quad (\text{denoted } \mathcal{C}_0 \prec\prec \mathcal{C})$$

and $\mathcal{C}_0$ is inductively connected with associated order ω_0 , called the *perturbation order*. For any multiple point P in $\mathcal{P}_i$, there is a unique chain of parents: $\tilde{P} = P_0 \subset P_1 \subset \cdots \subset P_i = P$ coming from $\mathcal{C}_0 \prec\prec \mathcal{C}_i$.

The algorithm. Let $\mathcal{A} = \{\ell_1, \dots, \ell_n\}$ be an arrangement with a m -perturbation $\mathcal{C}_0 \prec\prec \mathcal{C}(\mathcal{A}) = (\mathcal{A}, \mathcal{P}_{\mathcal{A}})$ and perturbation order ω_0 . Up to relabelling, we assume that $\omega_0(\ell_i) = i$. Furthermore, we can also assume that ℓ_1, ℓ_2, ℓ_3 and ℓ_4 are in generic position in $\mathcal{C}(\mathcal{A})$.

We define recursively two maps $\Lambda : \mathcal{A} \rightarrow \mathbb{N}$ and $\Theta : \mathcal{P}_{\mathcal{A}} \rightarrow \mathbb{N}$ as follows.

- (R1) For $i \in \{1, 2, 3, 4\}$, we fix $\Lambda(\ell_i) = 0$.
- (R2) For any $P \in \mathcal{C}(\mathcal{A})$, we fix $\Theta(\langle P \rangle) = 0$.
- (R3) For $i \in \{5, \dots, n\}$, the expression of $\Lambda(\ell_i)$ depends on the value $\tau_i(\mathcal{C}_0, \omega_0)$ as follows:
 - If $\tau_i(\mathcal{C}_0, \omega_0) = 0$, we fix $\Lambda(\ell_i) = 1$.
 - If $\tau_i(\mathcal{C}_0, \omega_0) = 1$, i.e. ℓ_i passes through a unique point P_0 in $(\mathcal{C}_0)_i$, we define:

$$\Lambda(\ell_i) := \begin{cases} 1 + \Lambda(\ell_j) & \text{if } \Lambda(\ell_j) = \Lambda(\ell_k), \\ \max(\Lambda(\ell_j), \Lambda(\ell_k)) & \text{otherwise.} \end{cases}$$

where ℓ_j and ℓ_k are two lines in the parent of P_0 .

- If $\tau_i(\mathcal{C}_0, \omega_0) = 2$, i.e. ℓ_i passes through two points P_0 and Q_0 in $(\mathcal{C}_0)_i$, we define

$$\Lambda(\ell_i) := \Theta(\langle P_0 \rangle) + \Theta(\langle Q_0 \rangle).$$

- (R4) For $i \in \{5, \dots, n\}$ and for any double point $P = \{\ell_i, \ell_j\}$ in $(\mathcal{C}_0)_i$, we define

$$\Theta(\langle P \rangle) = \Lambda(\ell_i) + \Lambda(\ell_j).$$

Theorem 2.3 ([GBVS23, Thm. 4.10]). *Let $\mathcal{A}$ be a line arrangement and assume that $\mathcal{C}(\mathcal{A})$ admits a m -perturbation $\mathcal{C}_0 \prec\prec \mathcal{C}(\mathcal{A})$. The following inequality holds:*

$$\#\text{CC}(\mathcal{M}(\mathcal{A})) \leq \prod_{i=1}^m (\Lambda(\ell_{i_1}) + \Lambda(\ell_{i_2}) + \Lambda(\ell_{i_3})).$$

where $\mathcal{C}_{i-1} \prec \mathcal{C}_i$ is the elementary perturbation at (ℓ_j, P) , and ℓ_{j_1}, ℓ_{j_2} are two lines contained in the parent of P in $\mathcal{C}_{i-1}$.

3. AN EXAMPLE

Let p be a prime number and fix a primitive p -root of unity ζ . Consider the arrangement $\mathcal{A}_p = \{\ell_1, \dots, \ell_{2p+2}\}$ with lines:

$$\ell_1: x - y = 0, \quad \ell_2: x - \zeta y = 0, \quad \ell_{2i+1}: x + \zeta^i z = 0 \quad \text{and} \quad \ell_{2i+2}: \zeta^{-i} y + z = 0,$$

for $i \in \{1, \dots, p\}$. The multiple points of $\mathcal{A}_p$ are the two points of multiplicity p :

$$\{\ell_3, \ell_5, \dots, \ell_{2p+1}\} \quad \text{and} \quad \{\ell_4, \ell_6, \dots, \ell_{2p+2}\},$$

and the $2p$ triple points given by:

$$\{\ell_1, \ell_{2i+1}, \ell_{2i+2}\} \quad \text{and} \quad \{\ell_2, \ell_{2i+2}, \ell_{[2i]+3}\}$$

for $i \in \{1, \dots, p\}$, where $[a]$ is the value of a modulo $2p$ such that $0 \leq [a] < 2p$.

Consider the elementary perturbation $\tilde{\mathcal{C}}(\mathcal{A}_p)$ on $\mathcal{C}(\mathcal{A}_p)$ at $(\ell_{2p+2}, \{\ell_2, \ell_3, \ell_{2p+2}\})$. Let ω_0 be the following order on $\tilde{\mathcal{C}}(\mathcal{A}_p)$:

$$(\ell_1, \dots, \ell_{2p+2}) \mapsto (5, 6, 1, 2, 3, 4, 7, 8, \dots, (2p+2)).$$

We have that $\tau(\tilde{\mathcal{C}}(\mathcal{A}_p), \omega_0) = (0, 0, 0, 0, 2, 1, 2, 2, \dots, 2, 2)$. So $\tilde{\mathcal{C}}(\mathcal{A}_p)$ is inductively connected, and thus it is a 1-perturbation of $\mathcal{C}(\mathcal{A}_p)$. Using the rules (R1)-(R2)-(R3)-(R4), we can compute that:

$$\Lambda_p: (\ell_1, \dots, \ell_{2p+2}) \mapsto (0, 1, 0, 0, 0, 0, 1, 1, 2, 2, \dots, p-2, p-2).$$

By Theorem 2.3, we obtain that $\mathcal{M}(\mathcal{A}_p)$ has at most $\Lambda_p(\ell_2) + \Lambda_p(\ell_3) + \Lambda_p(\ell_{2p+2}) = 1 + 0 + (p-2) = p-1$ connected components.

On the other hand, a direct computation shows that the $\dim_{\mathbb{C}} \mathcal{M}(\mathcal{A}) = 0$ and also $\mathcal{A}_p \in \mathcal{M}(\mathcal{A})$ for any choice of primitive p -root of unity ζ . We conclude that $\# \text{CC}(\mathcal{M}(\mathcal{A}_p)) = p-1$ and we have shown that the bound of Theorem 2.3 is sharp.

REFERENCES

- [GBVS23] Benoît Guerville-Ballé and Juan Viu-Sos. Connectedness and combinatorial interplay in the moduli space of line arrangements. Preprint, [arXiv:2309.00322](https://arxiv.org/abs/2309.00322) [math.AG], 2023.
- [NY12] Shateen Nazir and Masahiko Yoshinaga. On the connectivity of the realization spaces of line arrangements. *Ann. Sc. Norm. Super. Pisa Cl. Sci. (5)*, 11(4):921–937, 2012.
- [Ran89] Richard Randell. Lattice-isotopic arrangements are topologically isomorphic. *Proc. Am. Math. Soc.*, 107(2):555–559, 1989.
- [Sage] The Sage Developers. SageMath, the Sage Mathematics Software System (Version 10.2). <https://www.sagemath.org>, 2023.

(B. Guerville-Ballé)

URL: <http://www.benoit-guervilleballe.com/>

Email address: benoit.guerville-balle@math.cnrs.fr

(J. Viu-Sos)

Dpto. de Matemáticas e Informática (DMIAICN)

Universidad Politécnica de Madrid (Spain)

URL: <https://jviusos.github.io/>

Email address: juan.viu.sos@upm.es

ALGORITHMS ON JANET-LIKE BASES

RODRIGO IGLESIAS, MATTHIAS ORTH, AND EDUARDO SÁENZ-DE-CABEZÓN

ABSTRACT. Involutive divisions assign sets of *multiplicative/non-multiplicative variables* to each term of a set in the polynomial ring in n variables. These assignments give rise to involutive bases, which are a type of Gröbner basis with additional combinatorial properties. Some of these involutive divisions, in particular the so called Janet and Pommaret divisions have particularly interesting algebraic properties and are efficient tools for computing homological invariants of the ideal. A more compact version of involutive bases are known as involutive-like basis, which present some computational and structural advantages. We describe some properties of involutive-like bases and provide here algorithms for the completion of Janet and Janet-like monomial bases, as well as some comparisons among different approaches for such completions.

1. INVOLUTIVE DIVISIONS

Involutive bases were introduced in [2] as a type of Gröbner bases with additional combinatorial properties. Janet and Pommaret bases are particular kinds of involutive bases with strong relations to commutative algebra and algebraic geometry [3, 9, 10, 8].

Definition 1.1. An involutive division L is defined on the Abelian monoid $(\mathbb{N}_0^n, +)$, if for any finite set $\mathcal{N} \subset \mathbb{N}_0^n$ a subset $N_{L,\mathcal{N}}(\nu) \subseteq \{1, \dots, n\}$ of multiplicative indices is associated to every multi index $\nu \in \mathcal{N}$ such that the involutive cones $\mathcal{C}_{L,\mathcal{N}}(\nu) = \nu + \mathbb{N}_{N_{L,\mathcal{N}}(\nu)}^n$ satisfy the following two conditions.

- (1) If there exist two elements $\mu, \nu \in \mathcal{N}$ with $\mathcal{C}_{L,\mathcal{N}}(\mu) \cap \mathcal{C}_{L,\mathcal{N}}(\nu) \neq \emptyset$, either $\mathcal{C}_{L,\mathcal{N}}(\mu) \subseteq \mathcal{C}_{L,\mathcal{N}}(\nu)$ or $\mathcal{C}_{L,\mathcal{N}}(\nu) \subseteq \mathcal{C}_{L,\mathcal{N}}(\mu)$ holds.
- (2) If $\mathcal{N}' \subset \mathcal{N}$ then $N_{L,\mathcal{N}}(\nu) \subseteq N_{L,\mathcal{N}'}(\nu)$ for all $\nu \in \mathcal{N}'$.

Let $\mathbf{k}$ be some arbitrary field, we might of course also identify any multi index $\nu \in \mathbb{N}_0^n$ with the corresponding monomial $x^\nu \in R = \mathbf{k}[x_1, \dots, x_n]$. This identification makes the concept of division more intuitive. Let us also denote by $\mathcal{X}_{L,\mathcal{N}}(\nu)$ and $\overline{\mathcal{X}}_{L,\mathcal{N}}(\nu)$ the sets of multiplicative and non-multiplicative indices (or variables) respectively. We say that ν divides L -involutively μ , written $\nu|_{L,\mathcal{N}} \mu$, if $x^\nu|x^\mu$ (in the ordinary way), and furthermore $x^{\mu-\nu} \in \mathbf{k}[\mathcal{X}_{L,\mathcal{N}}(\nu)]$.

Definition 1.2. Let L be an involutive division and $\mathcal{N} \subset \mathbb{N}_0^n$ a finite set. Let furthermore $(\nu^{(1)}, \dots, \nu^{(t)})$ be a finite sequence of elements of $\mathbb{N}$ where every multi index $\nu^{(k)}$ with $k < t$ has a non-multiplicative index $j_k \in \overline{\mathcal{X}}_{L,\mathcal{N}}(\nu^{(k)})$ such that $\nu^{(k+1)}|_{L,\mathcal{N}} \nu^{(k)} + 1_{j_k}$. The division L is **continuous**, if any such sequence consists only of distinct elements, i. e. if $\nu^{(k)} \neq \nu^{(l)}$ for all $k \neq l$.

The first and third authors are partially funded by grant PID2020- 116641GB-I00 funded by MCIN/AEI/ 10.13039/501100011033. Furthermore, third author will be the one to give the talk at EACA 2024.

Continuous divisions allow constructive algorithmical completion processes, i.e., given a set of terms, there is an algorithmic way to complete it to an involutive basis. The Janet division is continuous, and furthermore **noetherian**, which means that every set of terms has a finite completion to an involutive basis. These two properties together make Janet division a particularly useful type of involutive division.

2. JANET-LIKE BASES

Janet-like bases for ideals in a polynomial ring were introduced by Gerdt and Blinkov [5, 6] as a generalization of the concept of Janet bases. Both Janet and Janet-like bases are, in turn, special types of Gröbner bases with additional combinatorial properties.

Both kinds of bases arise from a restriction of the divisibility relation between monomials via multiplicative and non-multiplicative variables (for Janet bases) and additionally, non-multiplicative *powers* (for Janet-like bases). We will mainly make use of the concept of non-multiplicative powers; they are best understood via their relation to Janet non-multiplicative variables. See [4, 9, 10] for an introduction to involutive bases, in particular Janet bases. See [7] for an account on the computational aspects of involutive-like bases.

Definition 2.1. Let $R = \mathbf{k}[x_1, \dots, x_n] = \mathbf{k}[\mathcal{X}]$ be a polynomial ring, and let x^μ be a monomial of R contained in a finite set of monomials $U \subset R$.

- (1) A variable x_i is *Janet non-multiplicative* for x^μ if there is a monomial $x^\nu \in U$ such that $\deg_{x_i}(x^\nu) > \deg_{x_i}(x^\mu)$ and $\deg_{x_j}(x^\nu) = \deg_{x_j}(x^\mu)$ for all $i < j \leq n$. We write $\overline{\mathcal{X}}_{JU}(x^\mu)$ for the set of all Janet non-multiplicative variables of x^μ .
- (2) Let $x_i \in \overline{\mathcal{X}}_{JU}(x^\mu)$, then there is a minimal positive integer p_i among the differences $\deg_{x_i}(x^\nu) - \deg_{x_i}(x^\mu)$ where $x^\nu \in U$ and $\deg_{x_j}(x^\nu) = \deg_{x_j}(x^\mu)$ for all $i < j \leq n$. We call $x_i^{p_i}$ a *Janet-like non-multiplicative power* of u and we write $\text{NMP}_{JU}(x^\mu)$ for the set of all non-multiplicative powers of u .
- (3) A monomial $x^\omega \in R$ is called a *Janet-like multiplier* for $x^\mu \in U$ if no element of $\text{NMP}_{JU}(x^\mu)$ divides x^ω (in the ordinary sense).

Janet-like bases are Gröbner bases that also respect the Janet-like divisibility restrictions for leading terms:

Definition 2.2. Let $I \subset R$ be a polynomial ideal and let $\prec$ be a monomial order on R . A finite set $H \subset I \setminus \{0\}$ is called a *Janet-like basis* of I if the leading terms of H are distinct and for any $f \in I \setminus \{0\}$, its leading term $\text{lt}_\prec(f)$ is Janet-like divisible by one of the leading terms of H , i.e., there is $h_\prec \in H$ such that $\text{lt}_\prec(f)/\text{lt}_\prec(h)$ is a Janet-like multiplier for $\text{lt}(h) \in \text{lt}(H)$. In which case we write $\text{lt}_\prec(h) \mid_{JL, \mathcal{H}} \text{lt}_\prec(f)$ to express that $\text{lt}_\prec(h)$ divides $\text{lt}_\prec(f)$ w.r.t. the Janet-like division.

3. ALGORITHMS

The noetherian property of the Janet division is inherited by the Janet-like division, and hence a completion algorithm is available for every monomial ideal, see [7]. In particular, a Janet-like basis is a more compact version of the Janet basis; furthermore, it contains enough information to recover the Janet basis. We have coined this process of recovering the Janet basis of an ideal from a given Janet-like basis as "filling in the gaps". Our tests

show that in general it is more efficient to build the Janet-like basis and then fill in the gaps to turn it into a Janet basis than it is to build the Janet basis directly.

In this work we will present a C++ implementation of an optimized algorithm for the Janet-like completion algorithm, using the computer algebra library CoCoALib[1]. The experiments show that this implementation is a lot more efficient when compared to the existing ones. The following is the algorithm that was implemented:

Algorithm 1 Monomial Janet-Like completion

Input: Minimal monomial generating set $G(I)$ of $I \subset R = \mathbf{k}[x_1, \dots, x_n]$.

Output: Minimal Janet-Like basis $\mathcal{H}$ of I .

```

1: SortLex( $G(I)$ ) ▷ Sorts the generators lexicographically in increasing order.
2:  $\mathcal{H} \leftarrow \{[g, NMP(g)] \mid g \in G(I)\}$  ▷  $NMP(g) \in \mathbb{N}_0^n \rightarrow$  Non-mult exponents of  $g$  in  $G(I)$ .
3:  $k \leftarrow \text{SizeOf}(G(I))$ 
4: for  $i = 1, \dots, k$  do
5:   for  $j = 1, \dots, n$  do
6:      $p_j \leftarrow NMP(h_i)_j$  ▷ Non-mult power of the variable  $x_j$  for  $h_i$  in  $\mathcal{H}$ .
7:     if  $p_j > 0$  then
8:        $\bar{h} \leftarrow h_i \cdot x_j^{p_j}$ 
9:        $\ell \leftarrow \min\{i \mid h_i \in \mathcal{H}, \bar{h} \prec_{lex} h_i\}$ 
10:       $flag \leftarrow true$ 
11:       $q \leftarrow i + 1$ 
12:      while  $q < \ell$  and  $flag$  do
13:        if  $h_q \mid_{JL} \bar{h}$  then
14:           $flag \leftarrow false$ 
15:        end if
16:         $q++$ 
17:      end while
18:      if  $flag$  then
19:        Insert( $([\bar{h}, NMP(\bar{h})], \ell, \mathcal{H})$ ) ▷ Adds new elem without altering lex order.
20:         $k++$ 
21:        for  $r = \ell, \dots, i$  do
22:          AdjustNMP( $h_r$ )
23:        end for
24:      end if
25:    end if
26:  end for
27: end for
28: return  $\mathcal{H}$ 

```

If one were to substitute line 8 of Algorithm 1 for " $\bar{h} \leftarrow h_i \cdot x_j$ ", then one would instead get the minimal Janet basis from the Algorithm. Alternatively, we propose the following algorithm for completing Janet Like bases into Janet bases:

Algorithm 2 Filling in the gaps method for Janet-Like basis**Input:** Minimal Janet-Like basis $\mathcal{H}$ of $I \subset R = \mathbf{k}[x_1, \dots, x_n]$.**Output:** Minimal Janet basis $\mathcal{J}$ of I .

```

1:  $\mathcal{J} \leftarrow \emptyset$ ,  $k \leftarrow \text{SizeOf}(\mathcal{H})$ 
2: for  $i = 1, \dots, k$  do
3:    $\overline{\mathcal{X}}_J(\overline{h}) \leftarrow \{x_j \mid x_j^{p_{j,i}} \in \text{NMP}(h_i)\}$   $\triangleright$  NMP are now non-mult powers of variables.
4:   for  $\forall x^p \in \text{Mon}(\mathbf{k}[\overline{\mathcal{X}}_J(\overline{h})] / \mathbf{k}[\text{NMP}_{JL}(h_i)])$  do
5:      $\overline{h} \leftarrow h_i \cdot x^p$ 
6:     PushBack( $[\overline{h}, \overline{\mathcal{X}}_J(\overline{h})]$ ,  $\mathcal{J}$ )
7:   end for
8: end for
9: return  $\mathcal{J}$ 

```

REFERENCES

- [1] J. Abbott and A. M. Bigatti. CoCoALib: a C++ library for doing Computations in Commutative Algebra. Available at <http://cocoa.dima.unige.it/cocoalib>.
- [2] Vladimir Gerdt and Yuri Blinkov. Involutive bases of polynomial ideals. *Mathematics and Computers in Simulation*, 45:519–542, 1998.
- [3] Vladimir Gerdt and Yuri Blinkov. Minimal involutive bases. *Mathematics and Computers in Simulation*, 45:543–560, 1998.
- [4] Vladimir P. Gerdt. On the relation between Pommaret and Janet bases. In Victor G. Ganzha, Ernst W. Mayr, and Evgenii V. Vorozhtsov, editors, *Computer Algebra in Scientific Computing*, pages 167–181, Berlin, Heidelberg, 2000. Springer Berlin Heidelberg.
- [5] Vladimir P. Gerdt and Yuri A. Blinkov. Janet-like Gröbner bases. *Computer algebra in scientific computing. 8th international workshop, CASC 2005, Kalamata, Greece*, page 184–195, September 12–16, 2005.
- [6] Vladimir P. Gerdt and Yuri A. Blinkov. Janet-like monomial division. *Computer algebra in scientific computing. 8th international workshop, CASC 2005, Kalamata, Greece*, page 174–183, September 12–16, 2005.
- [7] Amir Hashemi, Matthias Orth, and Werner M. Seiler. Recursive structures in involutive bases theory. *J. Symb. Comput.*, 118:32–68, 2023.
- [8] Rodrigo Iglesias and Eduardo Sáenz de Cabezón. Cellular structure of the Pommaret-Seiler resolution for quasi-stable ideals. *AAECC*, 2022.
- [9] Werner M. Seiler. A combinatorial approach to involution and δ -regularity I: Involutive bases in polynomial algebras of solvable type. *Applicable Algebra in Engineering, Communications and Computing*, 20:207–259, 2009.
- [10] Werner M. Seiler. A combinatorial approach to involution and δ -regularity II: Structure analysis of polynomial modules with Pommaret bases. *Applicable Algebra in Engineering, Communications and Computing*, 20:261–338, 2009.

Universidad de La Rioja
 Email address: roiglesi@unirioja.es

Universität Kassel
 Email address: morth@mathematik.uni-kassel.de

Universidad de La Rioja
 Email address: eduardo.saenz-de-cabezón@unirioja.es

SOME CLASSICAL RESULTS IN ALGEBRA NEEDING ONE OR SEVERAL CONSTRUCTIVE VERSIONS

HENRI LOMBARDI

ABSTRACT. We present some classical results in Algebra for which it should be relevant to give one or several constructive versions with constructive proofs.

INTRODUCTION

We present some classical results in Algebra for which it should be relevant to give one or several constructive versions with constructive proofs.

The Computer Algebra community has produced algorithms for several particular cases of the classical results we present and for which a constructive proof is needed in full generality.

A general constructive proof can also give useful hints for efficient algorithms.

Nevertheless many constructive theorems that use an hypothesis assuming a bound on the Krull dimension of a commutative ring, as e.g. those given in [1], remain nowadays without efficient implementation.

The constructive terminology we use can be found in [2] and [3].

1. MAXIMAL IDEALS, MAXIMAL SPECTRUM

- (1) Let K be a discrete field, the Jacobson radical of a finitely presented K -algebra is the nilradical.
- (2) Let $\mathbb{Z}$ be the ring of integers, the Jacobson radical of a finitely presented $\mathbb{Z}$ -algebra is the nilradical.
- (3) Decipher the “quick and dirty proof” of the Nullstellensatz given in [4, Eisenbud] Exercise 4.29 and an analogous argument in Exercise 4.31 (here he uses a cardinality argument).
- (4) Decipher the proof of the Nullstellensatz given by Eisenbud using the notion of Jacobson rings (rings where prime ideals are intersections of maximal ideals)

We need a constructive version of the following theorem, and a way to prove a (new?) constructive form of the Nullstellensatz.

Theorem 4.19 (Nullstellensatz—General form [5]). *Let R be a Jacobson ring. If S is a finitely generated R -algebra, then S is a Jacobson ring. Furthermore, if $\mathfrak{n} \subseteq S$ is a maximal ideal, then $\mathfrak{m} := \mathfrak{n} \cap R$ is a maximal ideal of R , and $S/\mathfrak{n}$ is a finite extension field of $R/\mathfrak{m}$.*

Let us recall [6] that a distributive lattice is called a *weakly Jacobson lattice* if each principal ideal is equal to its Jacobson radical, in other words if

$$(1) \quad \forall a, b \in T \quad [(\forall x \in T (a \vee x = 1 \Rightarrow b \vee x = 1)) \Rightarrow a \leq b]$$

Date: April 26, 2024.

A ring R is said to be *weakly Jacobson* if $\mathbf{Zar} R$ is a weakly Jacobson lattice. In other words for each finitely generated ideal $\mathfrak{a}$, the nilradical is equal to the Jacobson radical.

- (5) Two papers give interesting results for Noetherian rings whose maximal spectrum has dimension ≤ 1 .

Collect. Math. 48, 1–2 (1997), 85–96 (Proc. Journées Arithmétiques 1995) *A differential criterion for complete intersections*. B. de Smit.

Journal of Algebra 196, 520–531 (1997). *Finite Complete Intersection Algebras and the Completeness Radical*. B. de Smit and Lenstra.

It should be relevant to give constructive versions, perhaps non-Noetherian ones, using Heitmann dimension. The second paper is partly deciphered in ?.

2. INTEGRAL CLOSURES

- (1) ? **Theorem 4.14** (Emmy Noether). *If R is a finitely generated domain over a field or over the integers, and L is a finite extension field of the field of fractions of R , then the integral closure of R in L is a finitely generated R -module.*

Eisenbud says that this theorem can be proved using the Noether position theorem for a finitely presented algebra over a discrete field.

Theorem 4.14 in Eisenbud (by Emmy Noether) has been proved constructively or given with algorithms in Computer Algebra by many authors. See e.g. ? and ? in constructive mathematics, and ? and ? for Computer Algebra.

Nagata proved the theorem holds when replacing $\mathbb{Z}$ with any integrally closed Noetherian domain of dimension ≤ 2 .

A constructive proof of Nagata's theorem should be given assuming a constructive form of the hypotheses: the ring has to be strongly discrete and coherent and the extension of the field of fractions has to be finitely presented. These facts are always provable in classical mathematics. A constructive approach to Noetherian strongly discrete coherent rings can be found in ?.

Some constructive results use a stronger characterization of Noetherian rings than the one in ?. One finds a discussion on different constructive version of Noetherianity in ?.

3. ÉTALE ALGEBRAS

A *basic étale R -algebra* is an algebra $S = R[x_1, \dots, x_n] = R[X_1, \dots, X_n]/(f_1, \dots, f_n)$ when the Jacobian matrix is invertible in S .

Flatness.

- (1) Let $S = R[x_1, \dots, x_n] = R[X_1, \dots, X_n]/(f_1, \dots, f_n)$ be a basic étale R -algebra. Find a constructive proof that S is flat over R .
- (a) The result is equivalent to flatness of smooth algebras. The case of a standard smooth algebra implies the general case: a standard smooth presentation is given in the form $S = R[x_1, \dots, x_n] = R[X_1, \dots, X_n]/(f_1, \dots, f_r)$, $r \leq n$, such that the Jacobian matrix has its first $(r \times r)$ -minor invertible in S . A

smooth algebra is a finitely presented algebra where we have elements $s_1, \dots, s_\ell$ comaximal in S such that each $S[1/s_i]$ has a standard smooth presentation.

- (b) In ? Theorem 2.13, Chapter 17 gives a proof in the case of Noetherian rings without using ZMT. It seems easier to decipher constructively this proof than the proof in Stacks.
- (c) In ? the flatness is proved for “syntomic algebras”. In fact the crucial case is for “globally complete intersection algebras” with the following definition. Note: we think that this constructive definition is equivalent to the one given in Stacks. For a constructive approach to the notion of depth see ?.

A finitely presented algebra $\rho : R \rightarrow S$ is said a globally complete intersection when it is isomorphic to a $\mathbf{k}$ -algebra $R[X_1, \dots, X_n]/\langle f_1, \dots, f_r \rangle$ where the sequence $(f_1, \dots, f_r)$ has depth (true-grade) $\geq r$.

NB. The proof in Stacks is not constructive, and it does not use the ZMT.

- (2) Let $S = R[x_1, \dots, x_n] = R[X_1, \dots, X_n]/(f_1, \dots, f_s)$ be a finitely presented algebra. Find a constructive proof that if S is unramified and flat over R , then it is étale.

Local structure theorem. Following a suggestion of Laurent Moret-Bailly an R -algebra is said to be *standard* if it is isomorphic to an algebra $[R[X]/\langle f(X) \rangle][1/g(x)]$ (where $f, g \in R[X]$, f monic and x is X viewed in the quotient $R[X]/\langle f(X) \rangle = R[x]$).

- (1) Let $R = \mathbb{Z}[a_0, \dots, a_n]$ and the basic étale R -algebra

$$S = R[x, y] = R[X, Y]/\langle f(X), Yf'(X) - 1 \rangle$$

where $f = \sum_{k=0}^n a_k X^k$. Find comaximal elements $s_1, \dots, s_r$ in S such that each $S[1/s_k]$ is standard over R .

- (2) More generally, for an arbitrary basic étale R -algebra S , construct comaximal elements $s_1, \dots, s_r$ in S such that each $S[1/s_k]$ is standard over R . You can use constructive versions of the ZMT given in ?.

4. ARTINIAN RINGS

- (1) Let R be a strongly discrete coherent Noetherian zero-dimensional ring. It should be useful to find a constructive proof for a constructive form of the following classical result: *any finitely generated ideal has a finite length*.

5. REAL ALGEBRA

- (1) Consider the following classical result. Let R be a real closed field. A continuous semialgebraic function $f : R^n \rightarrow R$ is always a point with coordinates in R in a continuous family $\phi : S \times R^n \rightarrow R$ defined over $\mathbb{Q}$, and S is a semialgebraic closed set defined over $\mathbb{Q}$. So $f(\cdot) = \phi(s, \cdot)$ for an $s \in S$.

A simple example is given by

$$f(x, y) = \sqrt{a^2 x^2 + abxy + b^2 y^2},$$

which is the point with coordinates (a, b) in the continuous family

$$\phi(a, b, x, y) = \sqrt{a^2 x^2 + abxy + b^2 y^2}, \text{ with } S = R^2.$$

We need a constructive proof in the case of a *discrete* real closed field R . If we have such a constructive proof, we are able to give a constructively acceptable version of the usual definition given in classical mathematics for a semialgebraic continuous function $f : \mathbb{R}^n \rightarrow \mathbb{R}$. This usual definition, the pointwise continuity, requires a quantification over all elements of $\mathbb{R}^n$, which is not manageable constructively. So we can replace this classical definition by an equivalent one (equivalent in classical mathematics). This is the following one:

A semialgebraic continuous function $f : \mathbb{R}^n \rightarrow \mathbb{R}$ is a point with coordinates in $\mathbb{R}$ in a continuous family $\phi : S \times \mathbb{R}^n \rightarrow \mathbb{R}$ defined over $\mathbb{Q}$, where S is a semialgebraic closed set defined over $\mathbb{Q}$.

This is the same trick as the one given in ? where he defines continuous functions $f : \mathbb{R}^n \rightarrow \mathbb{R}$ as functions which are uniformly continuous over any closed bounded cube.

More details in <http://hlombardi.free.fr/Reels-geometriques.pdf>.

REFERENCES

- Mari-Emi Alonso, Thierry Coquand, and Henri Lombardi. Revisiting Zariski main theorem from a constructive point of view. *J. Algebra*, 406:46–68, 2014. doi: 10.1016/j.jalgebra.2014.02.003. URL <https://arxiv.org/abs/1602.00597>.
- Errett Bishop. *Foundations of constructive analysis*. McGraw-Hill, New York, 1967. URL <http://hlombardi.free.fr/Bishop.djvu>.
- Gabriele Buriola, Peter Schuster, and Ingo Blechschmidt. A constructive picture of Noetherian conditions and well quasi-orders. In *Unity of logic and computation*, volume 13967 of *Lecture Notes in Comput. Sci.*, pages 50–62. Springer, Cham, 2023.
- Thierry Coquand, Henri Lombardi, Claude Quitté, and Claire Tête. Résolutions libres finies. Méthodes constructives. Preprint, 2019. URL <https://arxiv.org/abs/1811.01873>.
- Thierry Coquand, Henri Lombardi, and Claude Quitté. Dimension de Heitmann des treillis distributifs et des anneaux commutatifs. In *Publications Mathématiques de l'Université de Franche-Comté Besançon. Algèbre et théorie des nombres. Années 2003–2006*. Besançon: Laboratoire de Mathématiques de Besançon, 2006, p. 57–100, version corrigée, 2022. URL <http://arxiv.org/abs/1712.01958>.
- CRing, collectif. *The CRing Project*. 2011. URL <https://math.uchicago.edu/~amatthew/cr.html>. A collaborative, open source textbook on commutative algebra.
- David Eisenbud. *Commutative algebra. With a view toward algebraic geometry*, volume 150. Berlin: Springer-Verlag, 1995.
- Patricia Gianni and Barry Trager. Integral closure of Noetherian rings. In *Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation (Kihei, HI)*, pages 212–216. ACM, New York, 1997.
- Gert-Martin Greuel, Santiago Laplagne, and Frank Seelisch. Normalization of rings. *J. Symbolic Comput.*, 45(9):887–901, 2010.
- Henri Lombardi and Claude Quitté. *Commutative algebra: constructive methods. Finite projective modules*. Algebra and applications, 20. Springer, Dordrecht, 2015a. URL <https://arxiv.org/abs/1605.04832>. Translated from the French (Calvage & Mounet, Paris, 2011, revised and extended by the authors) by Tania K. Roblot.
- Henri Lombardi and Claude Quitté. Théorème de de Smit et Lenstra, démonstration élémentaire. Preprint, 2015b. URL <https://arxiv.org/abs/1508.05589>.

- Ray Mines, Fred Richman, and Wim Ruitenburg. *A course in constructive algebra*. Universitext. Springer-Verlag, New York, 1988. doi: 10.1007/978-1-4419-8640-5.
- A. Seidenberg. Construction of the integral closure of a finite integral domain. II. *Proc. Amer. Math. Soc.*, 52:368–372, 1975.
- Stacks, collectif. *Stacks-Project*. 2022. URL <http://stacks.math.columbia.edu>.
- Gabriel Stolzenberg. Constructive normalization of an algebraic variety. *Bull. Am. Math. Soc.*, 74: 595–599, 1968.

Université de Franche-Comté, Laboratoire de Mathématiques de Besançon
Email address: `henri.lombardi@univ-fcomte.fr`

HAMMING WEIGHT DISTRIBUTIONS OF CODES THAT ARE LINEAR OVER A SUBFIELD

UMBERTO MARTÍNEZ-PENAS AND RUBÉN RODRÍGUEZ-BALLESTEROS

ABSTRACT. In this work, we study linear codes endowed with the block Hamming distance, or equivalently, codes with the classical Hamming distance that are linear over a subfield. This includes additive codes. We study MDS codes in this setting and define quasi-MDS (QMDS) codes and dually QMDS codes, which attain a more relaxed variant of the classical Singleton bound. We then provide MacWilliams equations and the weight distribution of dually QMDS codes, which only depends on their parameters and not on the codes. We conclude with a lower bound on the field size of dually QMDS codes.

1. SINGLETON BOUND AND QMDS CODES

In this section, we provide a relaxed version of the Singleton bound and define QMDS and dually QMDS codes. In the following, $\mathbb{F}_q$ denotes the finite field with q elements. We will also denote $[n] = \{1, 2, \dots, n\}$.

Definition 1.1. For $\mathbf{c} = (\mathbf{c}_1, \dots, \mathbf{c}_n) \in \mathbb{F}_q^{nr}$, where $\mathbf{c}_i \in \mathbb{F}_q^r$ for $i \in [n]$, its block Hamming weight is $\text{wt}_B(\mathbf{c}) = |\{i \in [n] : \mathbf{c}_i \neq 0\}|$. We define the block Hamming distance as $d_B(\mathbf{c}, \mathbf{d}) = \text{wt}_B(\mathbf{c} - \mathbf{d})$ for $\mathbf{c}, \mathbf{d} \in \mathbb{F}_q^{nr}$. The minimum distance of $\mathcal{C} \subseteq \mathbb{F}_q^{nr}$ is denoted by $d(\mathcal{C})$.

Clearly, $\mathbb{F}_q$ -linear codes in $\mathbb{F}_q^{nr}$ with the block Hamming distance are the same as $\mathbb{F}_q$ -linear codes in $\mathbb{F}_{q^r}^n$ with the classical Hamming distance. In the second case, $\mathbb{F}_{q^r}$ -linear codes would be included in our study. However, we will focus on duality based on the usual inner product in $\mathbb{F}_q^{nr}$, which is not $\mathbb{F}_{q^r}$ -bilinear when considered in $\mathbb{F}_{q^r}^n$. In particular, we consider a different duality than in the classical case. Moreover, notice that additive codes over general finite fields are included in our study by choosing q to be prime and r arbitrary.

From now on, a code means an $\mathbb{F}_q$ -linear code in $\mathbb{F}_q^{nr}$ and $\mathcal{C}^\perp \subseteq \mathbb{F}_q^{nr}$ denotes the dual of a code $\mathcal{C} \subseteq \mathbb{F}_q^{nr}$ with respect to the usual ($\mathbb{F}_q$ -bilinear) inner product in $\mathbb{F}_q^{nr}$. If $k = \dim(\mathcal{C})$ and $d = d(\mathcal{C})$, we say that $\mathcal{C} \subseteq \mathbb{F}_q^{nr}$ is a code of type $[n, r, k, d]$.

In Item 2 in the following proposition, we provide a relaxed form of the classical Singleton bound, which is Item 1. The proof is straightforward.

Proposition 1.2. *Let $\mathcal{C} \subseteq \mathbb{F}_q^{nr}$ be a code of type $[n, r, k, d]$. Then*

- (1) $k \leq r(n - d + 1)$, and
- (2) $d \leq n - \lceil \frac{k}{r} \rceil + 1 = n - \lfloor \frac{k-1}{r} \rfloor$.

As usual, a code is MDS if it attains the bound in Item 1. If $r \mid k$ (necessary for the code to be MDS), then both bounds coincide. However, when $r \nmid k$, the second bound may be attained but the first one cannot. This motivates the following definition.

La ponencia en el Encuentro EACA 2022 ha sido presentada por el segundo autor.

Definition 1.3. We say that a code of type $[n, r, k, d]$ is quasi-MDS or QMDS if $d = n - \lceil \frac{k}{r} \rceil + 1 = n - \lfloor \frac{k-1}{r} \rfloor$.

In particular, a classical MDS code is also QMDS. It is known that the dual of an MDS code is also MDS, also for the block Hamming distance [2]. However, it is not difficult to find an example of a QMDS code whose dual is not QMDS. This motivates the following.

Definition 1.4. A code is dually QMDS if both itself and its dual are QMDS.

2. MACWILLIAMS EQUATIONS

In this section, we obtain MacWilliams equations for the block Hamming distance, which are new to the best of our knowledge. The classical equations are obtained when $r = 1$.

Definition 2.1. Let $\mathcal{C}$ be a code of type $[n, r, k, d]$. The block weight distribution of $\mathcal{C}$ is defined as the numbers $A_j(\mathcal{C}) = |\{\mathbf{c} \in \mathcal{C} : \text{wt}_B(\mathbf{c}) = j\}|$, for $j = 1, \dots, n$.

Definition 2.2. Given $I \subseteq [n]$, we define $\pi_I : \mathbb{F}_q^{rn} \rightarrow \mathbb{F}_q^{r|I|}$ by $(\mathbf{c}_i)_{i \in [n]} \mapsto (\mathbf{c}_i)_{i \in I}$, for $\mathbf{c} \in \mathbb{F}_q^{rn}$. For a code $\mathcal{C} \subseteq \mathbb{F}_q^{rn}$, we define $\mathcal{C}^{\bar{I}} = \pi_I(\mathcal{C})$ (where $\bar{I} = [n] \setminus I$) and $\mathcal{C}_I = \pi_I(\mathcal{C} \cap \ker(\pi_I))$.

Theorem 2.3 (MacWilliams Equations). Let $\mathcal{C}$ be a code of type $[n, r, k, d]$, and let $A_j = A_j(\mathcal{C})$ and $A_j^\perp = A_j(\mathcal{C}^\perp)$, for $j = 1, \dots, n$. Then, for $v = 0, 1, \dots, n$,

$$\sum_{j=0}^{n-v} \binom{n-j}{v} A_j = q^{k-vr} \sum_{j=0}^v \binom{n-j}{n-v} A_j^\perp.$$

Proof. Denote $k = \dim(\mathcal{C})$ and $k_1 = \dim(\mathcal{C}^{\bar{I}})$. We have

$$(1) \quad \sum_{j=0}^{n-v} \binom{n-j}{v} A_j = \sum_{|I|=v} q^{k-k_1},$$

for $v = 0, \dots, n$, since both sides count the pairs $(\mathbf{c}, I)$ such that $\mathbf{c} \in \mathcal{C}$, $I \subseteq [n]$, $|I| = v$, and $\pi_I(\mathbf{c}) = 0$. First, for $\mathbf{c} \in \mathcal{C}$ such that $\text{wt}_B(\mathbf{c}) = j$, there are $\binom{n-j}{v}$ possible v -tuples of blocks of zeros within the word $\mathbf{c}$. Second, given $I \subseteq [n]$ with $|I| = v$, there are q^{k-k_1} words of $\mathcal{C}$ with zeros in the v blocks of I , since $\dim(\mathcal{C} \cap \ker(\pi_I)) = \dim(\mathcal{C}) - \dim(\pi_I(\mathcal{C})) = k - k_1$.

Next, the right-hand side of (1) equals

$$(2) \quad q^{k-vr} \sum_{|I|=v} \left| (\mathcal{C}^{\bar{I}})^\perp \right| = q^{k-vr} \sum_{|I|=v} \sum_{j=0}^v A_j \left((\mathcal{C}^{\bar{I}})^\perp \right) = q^{k-vr} \sum_{j=0}^v \sum_{|I|=v} A_j \left((\mathcal{C}^{\bar{I}})^\perp \right).$$

Now we prove that

$$(3) \quad \sum_{|I|=v} A_j \left((\mathcal{C}^\perp)_{\bar{I}} \right) = \binom{n-j}{v-j} A_j^\perp.$$

Both numbers count the possible pairs $(\mathbf{c}, I)$ such that $\mathbf{c} \in \mathcal{C}^\perp$, $\text{wt}_B(\mathbf{c}) = j$, $I \subseteq [n]$, $|I| = v - j$, and $\pi_I(\mathbf{c}) = 0$. First, for $I \subseteq [n]$ with $|I| = v - j$, there are $A_j \left((\mathcal{C}^\perp)_{\bar{I}} \right)$ words of $\mathcal{C}^\perp$ with weight j and with zeros in the $v - j$ blocks of I . Second, for $\mathbf{c} \in \mathcal{C}^\perp$ such that $\text{wt}_B(\mathbf{c}) = j$, there are $\binom{n-j}{v-j}$ possible $(v - j)$ -tuples of blocks of zeros within $\mathbf{c}$.

The theorem follows by using that (1) and (2) are equal, and applying (3) together with $(C^T)^\perp = (C^\perp)_T$ (see [3, Th. 1.5.7]). $\square$

3. WEIGHT DISTRIBUTION OF DUALY QMDS CODES

In this section, we compute the weight distribution of dually QMDS codes. As in the classical MDS case, the weight distribution of dually QMDS codes only depends on their parameters, i.e., two dually QMDS codes of the same parameters have the same distribution.

The following lemma can be proven as in [3, Cor. 1.4.14 & Th. 1.4.15].

Lemma 3.1. *Let $\mathcal{C}$ be a code of type $[n, r, k, d]$, G one of its generator matrices and H one of its parity-check matrices.*

- (1) *$\mathcal{C}$ is QMDS if and only if any $k \times r \lceil \frac{k}{r} \rceil$ submatrix of G formed by $\lceil \frac{k}{r} \rceil$ complete blocks has maximum rank k .*
- (2) *$\mathcal{C}$ is QMDS if and only if any $(nr - k) \times r(n - \lceil \frac{k}{r} \rceil)$ submatrix of H formed by $n - \lceil \frac{k}{r} \rceil$ complete blocks has maximum rank $r(n - \lceil \frac{k}{r} \rceil)$.*

Lemma 3.2. *Let $\mathcal{C}$ be a dually QMDS code of type $[n, r, k, d]$. Given $I \subseteq [n]$, we have*

$$\dim(\mathcal{C}_I) = \begin{cases} k - r|I| & \text{if } r|I| \leq k, \\ 0 & \text{if } r|I| > k. \end{cases}$$

Proof. First, if $r|I| > k$, then $|I| \geq \lceil \frac{k}{r} \rceil$. Since $\mathcal{C}$ is QMDS, we may apply Item 1 in Lemma 3.1 and we have $\dim(\pi_I(\mathcal{C})) = k$, thus $\dim(\mathcal{C}_I) = \dim(\mathcal{C}) - \dim(\pi_I(\mathcal{C})) = k - k = 0$.

Second, if $r|I| \leq k$, then $|I| \leq \lceil \frac{k}{r} \rceil = n - \lceil \frac{nr-k}{r} \rceil = n - \lceil \frac{\dim(\mathcal{C}^\perp)}{r} \rceil$. Since $\mathcal{C}^\perp$ is QMDS, we may apply Item 2 in Lemma 3.1 to a generator matrix of $\mathcal{C}$ (i.e., a parity-check matrix of $\mathcal{C}^\perp$), and we have $\dim(\pi_I(\mathcal{C})) = r|I|$, thus $\dim(\mathcal{C}_I) = \dim(\mathcal{C}) - \dim(\pi_I(\mathcal{C})) = k - r|I|$. $\square$

Using Lemma 3.2, we may prove the main result of this section.

Theorem 3.3. *Let $\mathcal{C}$ be a dually QMDS code of type $[n, r, k, d]$. Then $A_0 = 1$, $A_j = 0$ for all $j \in [d-1]$, and if $d \leq j \leq n$, then*

$$A_j = \binom{n}{j} \sum_{i=0}^{j-d} (-1)^i \binom{j}{i} (q^{k-r(n-j+i)} - 1).$$

Proof. The only non-trivial cases are those with $d \leq j \leq n$. By Lemma 3.2, for $I \subseteq [n]$,

$$(4) \quad |\mathcal{C}_I| = \begin{cases} q^{k-r|I|} & \text{if } r|I| \leq k, \\ 1 & \text{if } r|I| > k. \end{cases}$$

Define $N_t = \sum_{|I|=t} |\mathcal{C}_I|$. N_t counts the number of words in $\mathcal{C}$ with block weight $\leq n - t$, counted once for each $\mathcal{C}_I$ they appear in, where $|I| = t$. By (4), we have

$$N_t = \begin{cases} \binom{n}{t} q^{k-rt} & \text{if } rt \leq k, \\ \binom{n}{t} & \text{if } rt > k. \end{cases}$$

By the inclusion-exclusion principle, we deduce that

$$A_j = \sum_{i=0}^j (-1)^i \binom{n-j+i}{i} N_{n-j+i} =$$

$$\sum_{i=0}^{\lfloor \frac{k}{r} \rfloor + j - n} (-1)^i \binom{n-j+i}{i} \binom{n}{n-j+i} q^{k-r(n-j+i)} + \sum_{i=\lfloor \frac{k}{r} \rfloor + j - n + 1}^j (-1)^i \binom{n-j+i}{i} \binom{n}{n-j+i}$$

Using $\binom{n-t}{i} \binom{n}{n-t} = \binom{n}{t-i} \binom{t-i}{i}$ and $\sum_{i=j-v+1}^j (-1)^i \binom{j}{i} = -\sum_{i=0}^{j-v} (-1)^i \binom{j}{i}$, we obtain

$$A_j = \binom{n}{j} \sum_{i=0}^{\lfloor \frac{k}{r} \rfloor + j - n} (-1)^i \binom{j}{i} (q^{k-r(n-j+i)} - 1),$$

when $d \leq j \leq n$. The formula in the theorem now easily follows by using $d = n - \lceil \frac{k}{r} \rceil + 1$. $\square$

As a consequence, we deduce the following lower bounds on the field size of dually QMDS codes, extending the known bounds for MDS codes [3, Cor. 7.4.3] (recall that tighter bounds for MDS codes hold for prime fields [1], coinciding with the MDS conjecture).

Corollary 3.4. *Let $\mathcal{C}$ be a dually QMDS code of type $[n, r, k, d]$ and denote $d^\perp = d(\mathcal{C}^\perp)$. Assume that $k = r\lfloor \frac{k}{r} \rfloor + r'$, where $0 < r' < r$.*

- (1) *If $k > r$, then $d = n - \lfloor \frac{k}{r} \rfloor \leq q^r - 1 + \frac{q^r - 1}{q^{r'} - 1}$.*
- (2) *If $k < r(n - 1)$, then $d^\perp = \lceil \frac{k}{r} \rceil \leq q^r - 1 + \frac{q^r - 1}{q^{r'} - 1}$.*

In particular, if $r < k < r(n - 1)$, then $n \leq 2q^r + 2\frac{q^r - 1}{q^{r'} - 1} - 3$.

Proof. We only need to prove Item 1 by duality. It is easy to see that $\lceil \frac{k}{r} \rceil = \lfloor \frac{k}{r} \rfloor + 1$ since $0 < r' < r$. In particular, we have $\lceil \frac{k}{r} \rceil = \lfloor \frac{k}{r} \rfloor + 1 \geq 2$ since $k > r$, which means that $d = n - \lceil \frac{k}{r} \rceil + 1 \leq n - 1$. Thus we may consider A_{d+1} . By Theorem 3.3, we have that

$$A_{d+1} = \binom{n}{d+1} (q^{k+r(d+1-n)} - 1 - (d+1)(q^{k+r(d-n)} - 1)) \geq 0.$$

Using that $k + r(d - n) = k - r\lfloor \frac{k}{r} \rfloor = r'$, the last inequality is equivalent to $q^{r'+r} - 1 \geq (d+1)(q^{r'} - 1)$. Therefore

$$d+1 \leq \frac{q^{r'+r} - 1}{q^{r'} - 1} = \frac{q^{r'+r} - q^r + q^r - 1}{q^{r'} - 1} = q^r + \frac{q^r - 1}{q^{r'} - 1}.$$

Finally, $n \leq 2q^r + 2\frac{q^r - 1}{q^{r'} - 1} - 3$ follows by combining Items 1 and 2 with $\lceil \frac{k}{r} \rceil = \lfloor \frac{k}{r} \rfloor + 1$. $\square$

REFERENCES

- [1] S. Ball. On sets of vectors of a finite vector space in which every subset of basis size is a basis. *Journal of the European Mathematical Society*, 14(3):733–748, 2012.
- [2] S. Ball, G. Gamboa, and M. Lavrauw. On additive MDS codes over small fields. *Advances in Mathematics of Communications*, 17(4):1–17, 2023.
- [3] W. C. Huffman and V. Pless. *Fundamentals of error-correcting codes*. Cambridge University Press, Cambridge, 2003.

University of Valladolid

Email address: `umberto.martinez@uva.es`

University of Valladolid

Email address: `ruben.rodriguez22@estudiantes.uva.es`; `rubenrb@iesgalileo.es`

STABLE RANK ANALYSIS APPLIED TO SEMI-SUPERVISED LEARNING

DANIEL MIGUEL, ANDREA GUIDOLIN, AND ANA ROMERO

ABSTRACT. We illustrate how methods from topological data analysis can be applied to semi-supervised learning. Specifically, we consider invariants called stable ranks to compare the unlabeled points of a dataset to the labeled points, with the aim of extending the classification. We apply our method to different datasets, and we discuss the possibilities offered by the use of stable ranks.

INTRODUCTION

Persistent homology [7], one of the main methods of topological data analysis (TDA), summarizes the emergence and disappearance of topological features in a filtration of topological spaces, producing an invariant that has found numerous applications in data analysis. In TDA, when the starting point is a set endowed with a notion of distance (e.g. a metric), the first step usually consists in representing the data as a filtration of simplicial complexes, using for example the Vietoris–Rips or the Čech filtration. Applying homology (in a fixed degree and with coefficients in a fixed field $\mathbb{F}$) to the filtration, one obtains a persistence module, that is a functor $M : [0, \infty) \rightarrow \mathbf{vect}_{\mathbb{F}}$ from the poset of nonnegative real numbers to the category of finite dimensional $\mathbb{F}$ -vector spaces. The decomposition of persistence modules into indecomposables, each of which can be described by a pair of real numbers, provides an invariant which completely characterizes the persistence module (up to isomorphism) and which is usually represented as a barcode or as a persistence diagram.

Since the space of all persistence modules lacks a linear structure, in applications to data analysis the invariant of persistent homology is often further transformed. For example, several vectorization methods have been proposed (e.g. persistence landscapes [4], persistence images [1]), each consisting in a function from the space of all persistence modules to a vector space. Using these vectorization methods, one gains access to a wealth of well-developed statistical methods that are useful for further analysis based on the invariants of persistent homology.

The stable rank method [8, 5] transforms a persistence module into a nonincreasing piecewise linear function from $[0, \infty)$ to $\mathbb{N}$, called a stable rank. Importantly, stable ranks depend on a choice of a pseudometric between persistence modules, and satisfy a stability result with respect to it [8]. Starting from the barcode of a persistence module, stable ranks can be efficiently computed with respect to several pseudometrics between persistence

Partially funded by grant PID2020-116641GB-I00, MICIU/AEI/10.13039/501100011033, project Inicia 2023/02 funded by La Rioja Government (Spain), by the dBrain collaborative project at Digital Futures at KTH, by the Strategic Support grant of the Digitalisation Platform at KTH and by the Data Driven Life Science (DDLS) program funded by the Knut and Alice Wallenberg Foundation.

The talk at the meeting EACA 2024 has been given by the first author.

modules, including the interleaving distance [5], Wasserstein distances [3], and a large family of distances involving some transformations of the domain $[0, \infty)$ of the persistence module, called contours [5]. Considering a large space of distances makes stable ranks a very flexible method, which can be effectively adapted to the task at hand.

Our work applies TDA methods to semi-supervised learning. In particular, we consider a situation similar to [6], and use stable ranks for our analysis. Given a dataset and two subsets whose points are labeled, we consider the task of labeling the rest of the points. To achieve the classification, we analyze the topological structure of the already-labeled subsets via the stable ranks, which we then use for a comparison with the remaining points.

1. A FIRST APPROACH

Our input is a dataset of points in a metric space. Some of the points are already labeled. We call them zeros and ones. Given an unlabeled point p , we represent it as a piecewise constant function obtained via the stable rank method. Our goal is to extend the labeling to all the points of the dataset.

We describe here the general strategy we considered for the task, followed by details on the specific choices we made.

1. First, we notice that we have two different labeled sets, so we decide to **compute two functions**: one with respect to the zeros and one with respect to the ones.
2. Following a procedure for topological analysis described in [2], we fix an unlabeled point p and repeatedly subsample the set of points of interest (for example, the zeros). The subsampling procedure, which involves a choice of a **size of the sample**, is carried out using a chosen **probability distribution** on the distances of the points of interest from the fixed point p .
3. We compute the stable rank of that set of sampled points. This involves a choice of a **filtration, contour function, homological degree** and **field of coefficients**.
4. In order to obtain a more robust invariant associated with any fixed point p , we repeat the subsampling procedure 100 times, and we compute the average stable rank. We get two piecewise constant functions, denoted $sr0_p$ and $sr1_p$ (to be read "average stable rank of the zeros/ones with respect to p ").
5. To assign a label to the point p , we would like to compare $sr0_p$ with some functions $sr0_0$ and $sr0_1$ (and similarly for $sr1_p$).
6. For each point with label zero we repeat the process that has been described in steps 2-4, obtaining again two functions. We chose to consider the **average for all the zeros** to obtain only two functions, called $sr0_0$ and $sr1_0$. Similarly we obtain $sr0_1$ and $sr1_1$.
7. We choose a distance d between piecewise constant functions and assign the zero label to p if

$$d_0 := d(sr0_0, sr0_p) + d(sr1_0, sr1_p) < d(sr1_1, sr1_p) + d(sr0_1, sr0_p) =: d_1.$$

We label p as one if the inequality above is in the other direction.

8. Finally, following [6] we can also **set a threshold** to be used at the moment of assigning a label, so that a point p is not labeled in cases of high uncertainty. More specifically, if the ratio between $\max(d_0, d_1)$ and $d_0 + d_1$ is smaller than a threshold **th**, we do not label the point.

In our case, as first contact with the problem, we have made the following choices:

- The size of the sample is half the number of labeled points.
- The probability distribution of the distance from a fixed point p is a normal distribution centered at 0 and with standard deviation proportional to the maximal distance of a labeled point from p .
- The contour function is the standard contour (see [8, 2, 5]).
- The homological degree is zero, and the field of coefficients is $\mathbb{Z}_2$. We use the python package Ripser to compute the barcodes of persistence modules obtained via the Vietoris-Rips filtration.
- We have set the same thresholds as in the original work [6].
- We have picked the distance l_2 to measure the differences between stable ranks.

Again, following the pipeline of the original work [6], we use the same datasets (in order to compare the results) to apply our methods. We train Support Vector Machine (SVM) and Random Forest (RF) classifiers with the labeled data. We present the accuracy results in Figure 1 for some specific thresholds (th), including the base results obtained before the training.

	Banknote		Breast Cancer		Ionosphere		Prima indian		Sonar	
	SVM	RF	SVM	RF	SVM	RF	SVM	RF	SVM	RF
base	97.0	88.6	89.3	96.1	80.0	93.3	65.7	60.9	61.3	64.5
no th	87.9	89.0	89.3	90.3	76.7	86.7	66.4	66.4	58.1	54.8
th=0.2	84.4	87.1	36.0	36.0	76.7	86.7	66.4	66.4	58.1	54.8
th=0.4	88.2	86.0	36.0	36.0	76.7	76.7	66.4	66.4	58.1	54.8
th=0.6	90.5	89.0	36.0	36.0	80.0	96.7	66.4	67.8	54.8	58.1
th=0.8	89.8	87.5	36.0	36.0	80.0	93.3	65.7	60.8	61.2	64.5

FIGURE 1. Accuracy results for the SVM and RF classifiers. Best result for each dataset is highlighted in bold face. The programs can be found at <https://github.com/DanielMT1997/EACA2024>

2. INTRODUCING A k -NEAREST NEIGHBOURS LABELING

As part of an ongoing work, we are refining the previous pipeline on several points. We believe that the main issue of the previous approach is point 6., taking the average of all the already labeled points to obtain $sr0_0$, $sr1_1$, $sr0_1$, and $sr1_0$. Instead, we propose to keep, for each labeled point q , the functions $sr0_0^q$ and $sr1_0^q$ (if it is a zero) and $sr1_1^q$ and $sr0_1^q$ (if it is a one).

Consequently, for point 7., we compute for each zero the distance

$$d(sr0_0^q, sr0_p) + d(sr1_0^q, sr1_p),$$

and for each one the distance

$$d(sr1_1^q, sr1_p) + d(sr0_1^q, sr0_p).$$

We choose an odd k , and we order all the previous distances for all the labeled points. We label p as zero if among the k smallest distances there are more zeros, and we label it to be a 1 otherwise.

Moreover, we have implemented, for each dataset, a set of contour functions, in order to take advantage of the flexibility of stable ranks, whose definition depends on the choice of a pseudometric between persistence modules (here the different contours induce different pseudometrics, hence different stable ranks). Finally, we are also implementing the previous method combining homological degrees zero and one. In this case, we obtain four functions for each point (two for each homological degree). The results of the implementation are available at <https://github.com/DanielMT1997/EACA2024>.

3. CONCLUSIONS AND FURTHER WORK

In our first approach, despite choosing standard parameters, we have managed to improve the base results for two of the five datasets. The results in general are slightly worse than in the original work [6], but the approach does not take advantage of the additional flexibility of stable rank. However, we still managed to improve their best accuracy result for the fourth dataset. We believe that our accuracy can be improved with a systematic optimization of the parameters involved. In particular, we plan to search the large space of contours by randomly generating and selecting contours or via a gradient descent technique as in [3].

In the second approach, we carry out a more exhaustive analysis to determine which type of contours are best for semi-supervised learning, and we consider a different labeling method. So far, our results have not been any better. Therefore, as future work, we plan to refine the previous method in order to improve the outcomes.

REFERENCES

- [1] *Persistence images: A stable vector representation of persistent homology*, HENRY ADAMS ET AL., Journal of Machine Learning Research, 18, 1–35, 2017.
- [2] *Data, geometry and homology*, JENS AGERBERG, WOJCIECH CHACHÓLSKI, AND RYAN RAMANUJAM, arXiv preprint arXiv:2203.08306, 2022.
- [3] *Algebraic Wasserstein distances and stable homological invariants of data*, JENS AGERBERG, ANDREA GUIDOLIN, ISAAC REN, AND MARTINA SCOLAMIERO, arXiv preprint arXiv:2301.06484, 2023.
- [4] *Statistical topological data analysis using persistence landscapes*, PETER BUBENIK, Journal of Machine Learning Research, 16, 77–102, 2015.
- [5] *Metrics and stabilization in one parameter persistence*, WOJCIECH CHACHÓLSKI AND HENRI RIIHIMAKI, SIAM Journal on applied Algebra and Geometry, 4(1), 69–98, 2020.
- [6] *Semi-Supervised Machine Learning: a Homological Approach*, ADRIÁN INÉS, CÉSAR DOMÍNGUEZ, JÓ-NATHAN HERAS, GADEA MATA, AND JULIO RUBIO, Proceedings of the XVII EACA, 109–112, 2022. arXiv [Cs.LG]. Retrieved from <https://arxiv.org/abs/2301.11658>.
- [7] *Persistence theory: from quiver representations to data analysis*, STEVE Y. OUDOT, American Mathematical Soc., 2017.
- [8] *Multidimensional persistence and noise*, MARTINA SCOLAMIERO, WOJCIECH CHACHÓLSKI, ANDERS LUNDMAN, RYAN RAMANUJAM, AND SEBASTIAN ÖBERG, Foundations of Computational Mathematics, 17, 1367–1406, 2017.

Daniel Miguel, University of La Rioja
Email address: damigutr@unirioja.es

Andrea Guidolin, KTH Stockholm
Email address: guidolin@kth.se

Ana Romero, University of La Rioja
Email address: ana.romero@unirioja.es

A NEW CRITERION FOR THE POSITIVITY OF SYMMETRIC POLYNOMIALS OF DEGREE 6

ROMUALDO E. MIRA AND ANTONIO DÍAZ-CANO

ABSTRACT. Since 1888, when Hilbert published his fundamental result on the relationship between non-negative polynomials and sums of squares, cf. [1], the Real Algebraic Geometry has undergone an extraordinary development, especially in the last decades. The aim of this note is to give a new positivity criterion for symmetric polynomials of degree 6. This criterion says that a real symmetric polynomial of degree 6 in n variables that satisfy certain property is non-negative on $\mathbb{R}^n$ if and only if it is non-negative on the subset of points of $\mathbb{R}^n$ with two distinct components.

INTRODUCTION

One of the central problems in Real Algebraic Geometry is that of the non-negativity of polynomials. In this note we consider symmetric polynomials, that is, polynomials invariant under the permutation of the variables. Symmetric polynomials are used extensively in many fields, see for example [2] and the many references therein.

In the paper [5] Timofte proved that a symmetric polynomial of degree d in n variables is non-negative on $\mathbb{R}^n$ if and only if it is non-negative on the subset of points with at most $\max\{\lfloor d/2 \rfloor, 2\}$ distinct components. The purpose of this note is to prove an analogous result for polynomials of degree 6 but reducing the number of distinct components from $\lfloor d/2 \rfloor = 3$ to 2. We will closely follow the approach of Riener, cf. [3], who proved the results of Timofte in an elementary way which is more convenient for our purpose.

The polynomial $F \in \mathbb{R}[X] := \mathbb{R}[X_1, \dots, X_n]$ is said to be symmetric if for any $\sigma \in S_n$ we have $F(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = F(X_1, \dots, X_n)$. The ring of symmetric polynomials will be denoted by $\mathbb{R}[X]^{S_n}$. Given a point $x \in \mathbb{R}^n$ the number of distinct components of x will be denoted as $n(x) := \#\{x_1, \dots, x_n\}$ and the set of points with at most k distinct components by $A_k := \{x \in \mathbb{R}^n \mid n(x) \leq k\}$. The following theorem is proved in [3]

Theorem 0.1. *Let $F_0, F_1, \dots, F_m \in \mathbb{R}[X]^{S_n}$ be symmetric polynomials, $d = \deg F_0$, $K = \{x \in \mathbb{R}^n \mid F_1(x) \geq 0, \dots, F_m(x) \geq 0\}$ and $k := \max\{2, \lfloor d/2 \rfloor, \deg F_1, \dots, \deg F_m\}$, then*

$$\inf_{x \in K} F_0(x) = \inf_{x \in K \cap A_k} F_0(x)$$

An immediate corollary of this theorem is the following:

Corollary 0.2 (Half-degree principle). *Let $F_0 \in \mathbb{R}[X]^{S_n}$ be of degree d and let $k := \max\{2, \lfloor d/2 \rfloor\}$. Then $F_0 \geq 0$ holds on $\mathbb{R}^n$ if and only if it holds on A_k .*

Furthermore, there is $x \in \mathbb{R}^n$ with $F_0(x) = 0$ if and only if there is $x \in A_k$ with $F_0(x) = 0$.

The second author has been partially supported by Grupo UCM 910444.

The talk at the meeting EACA 2024 will be given by the first author.

In particular, the latter result says that checking whether a symmetric polynomial F of degree 4 is positive semidefinite (*psd* for short) can be reduced to checking whether another polynomial, say $\tilde{F}$, in two variables (not necessarily symmetric) is also *psd*. By Hilbert's theorem, cf. [1], the latter is equivalent to checking whether $\tilde{F}$ is *sos* (a sum of squares), problem for which efficient algorithms exist. The main result of this note is:

Theorem 0.3 (Third-degree principle for sextics). *Let $F \in \mathbb{R}[X_1, X_2, X_3]^{S_3}$ be a symmetric polynomial of degree 6 and suppose that $F(1, e^{2\pi i/3}, e^{-2\pi i/3}) \leq 0$ then $F \geq 0$ on $\mathbb{R}^3$ if and only if $F \geq 0$ on A_2 . In particular, if F is homogeneous, F is positive semidefinite if and only if $\tilde{F}(X_1, X_2) := F(X_1, X_2, X_2)$ is *psd* if and only if $\tilde{F}$ is *sos*.*

The result can be generalized for any number of variables as we shall see below. The proof of these results relies on the fact that the set of zeros of symmetric polynomials can be seen as a variety in the orbit space of S_n , which agrees with the coefficient space of monic real univariate hyperbolic polynomials, i.e., polynomials with only real roots.

1. DEFINITIONS AND PRELIMINARIES

It is well known that the elementary symmetric polynomials, cf. [4], defined as $e_k := \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} X_{i_1} \dots X_{i_k}$, for $k = 1, \dots, n$, are algebraic independent generators of the ring $\mathbb{R}[X]^{S_n}$, so that for any $F \in \mathbb{R}[X]^{S_n}$ there is a unique $G \in \mathbb{R}[X]$ such that $F = G(e_1, \dots, e_n)$. Then we have that

$$\inf_{x \in \mathbb{R}^n} F(x) = \inf_{z \in \mathcal{H}} G(z)$$

where $\mathcal{H} := \{(e_1(x), \dots, e_n(x)) \mid x \in \mathbb{R}^n\}$. By the classical Vieta formula

$$f = \prod_{i=1}^n (T - x_i) = T^n - e_1(x)T^{n-1} + \dots + (-1)^n e_n(x)$$

we can write $\mathcal{H}$ as the set $\{z \in \mathbb{R}^n \mid T^n - z_1 + \dots + (-1)^n z_n \text{ has only real roots}\}$. Moreover, the sets $A_k = \{x \in \mathbb{R}^n \mid n(x) \leq k\}$ can be identified with $\mathcal{H}^k := \{z \in \mathcal{H} \mid T^n - z_1 T^{n-1} + \dots + (-1)^n z_n \text{ has at most } k \text{ real roots}\}$. Polynomials in $\mathbb{R}[T]$ with only real roots are called *hyperbolic* and one important result that shall be used below, cf. [3], is the following

Proposition 1.1. *Let $f \in \mathbb{R}[T]$ be a hyperbolic polynomial of degree d with k distinct roots.*

a) If $k = d$, then for any polynomial g of degree at most d there exists $\delta > 0$ such that for $-\delta < \epsilon < \delta$ the polynomials $f + \epsilon g$ are also hyperbolic with d distinct roots.

b) If $k < d$, then for each $1 \leq s \leq k$, there is a polynomial g_s of degree $n - s$ and a $\delta_s > 0$ such that for $0 < |\epsilon| < \delta_s$ the polynomials $f + \epsilon g$ are hyperbolic with strictly more distinct roots than f .

When we fix some of the coefficients of the hyperbolic polynomials we have to consider the subsets $\mathcal{H}(a_1, \dots, a_s) = \{z \in \mathcal{H} \mid z_1 = a_1, \dots, z_s = a_s\}$ and $\mathcal{H}^k(a_1, \dots, a_s) = \{z \in \mathcal{H}^k \mid z_1 = a_1, \dots, z_s = a_s\}$. Two important properties are, cf. [3],

Proposition 1.2. *Let $s \geq 2$. Then*

a) The subset $\mathcal{H}(a_1, \dots, a_s)$ is compact.

b) If $\mathcal{H}(a_1, \dots, a_s) \neq \emptyset$ there is some $z \in \mathcal{H}^s(a_1, \dots, a_s)$.

2. THIRD DEGREE PRINCIPLE FOR POLYNOMIALS OF DEGREE 6

In this section we focus on symmetric polynomials of degree 6 and the first result has to do with the way a polynomial of degree 6 can be written in terms of the elementary symmetrical forms.

Proposition 2.1. *Let $F \in \mathbb{R}[X]^{S_n}$ be a symmetric polynomial of degree 6. Then there is a unique polynomial $G \in \mathbb{R}[Z]$ such that*

$$F(X) = G(e_1, \dots, e_n) = ae_3^2 + be_6 + g_1(e_1)e_5 + g_2(e_1, e_2)e_4 + g_3(e_1, e_2)e_3 + g_4(e_1, e_2)$$

for some $a, b \in \mathbb{R}$ and polynomials $g_1, \dots, g_4$.

The coefficient a plays an important role in the following, so we will say that the polynomial F satisfies **condition (A)** if $a \leq 0$. In the case F is homogeneous condition (A) is equivalent to the inequality $F(1, e^{2\pi i/3}, e^{-2\pi i/3}, 0, \dots, 0) \leq 0$ (just note that $1, e^{2\pi i/3}$ and $e^{-2\pi i/3}$ are the cube roots of unity so $e_1(z) = e_2(z) = 0$ and $e_3(z) = 1$).

Proposition 2.2. *Let $F \in \mathbb{R}[X]^{S_n}$ be a symmetric polynomial of degree 6 that satisfies condition (A) and suppose $\mathcal{H}(a_1, a_2) \neq \emptyset$. Let M denote the set of minimizers of the quadratic problem*

$$(P) : \begin{cases} \min az_3^2 + bz_6 + cz_5 + dz_4 + fz_3 + r \\ z = (z_1, \dots, z_n) \in \mathcal{H}(a_1, a_2) \end{cases}$$

with $c = g_1(a_1)$, $d = g_2(a_1, a_2)$, $f = g_3(a_1, a_2)$, $r = g_4(a_1, a_2)$. Then $M \cap \mathcal{H}^2(a_1, a_2) \neq \emptyset$.

Proof. Note that $H(a_1, a_2)$ is a compact set (proposition 1.2) and $f(z) = az_3^2 + bz_6 + cz_5 + dz_4 + fz_3 + r$ is a continuous function of z , thus there is at least one minimizer z .

In case $a = b = c = d = f = 0$, every point in $\mathcal{H}(a_1, a_2)$ is a minimizer but proposition 1.2 says that there is some $z \in \mathcal{H}^2(a_1, a_2)$ and we are done. Otherwise, take a minimizer z such that $\tilde{f}(t) = t^6 - a_1t^5 + a_2t^4 - z_3t^3 + z_4t^2 - z_5t + z_6$ has the maximal number k of distinct roots.

In case $k = 6$, by proposition 1.1, for small enough values of ϵ_i the polynomial $g_\epsilon(t) = t^6 - a_1t^5 + a_2t^4 - (z_3 + \epsilon_3)t^3 + (z_4 + \epsilon_4)t^2 - (z_5 + \epsilon_5)t + (z_6 + \epsilon_6)$ also has $k = 6$ distinct real roots. But z cannot be a minimizer since for some ϵ_i , $az_3^2 + bz_6 + cz_5 + dz_4 + fz_3 + r > a(z_3 + \epsilon_3)^2 + b(z_6 + \epsilon_6) + c(z_5 + \epsilon_5) + d(z_4 + \epsilon_4) + f(z_3 + \epsilon) + r$, which is a contradiction.

Finally, suppose $3 \leq k < 6$. Using again proposition 1.1, there are y_j , $j = 3, \dots, 6$ such that the polynomial $g_\epsilon(t) = t^6 - a_1t^5 + a_2t^4 - (z_3 + \epsilon y_3)t^3 + (z_4 + \epsilon y_4)t^2 - (z_5 + \epsilon y_5)t + (z_6 + \epsilon y_6)$ has strictly more distinct roots than k . But for appropriate ϵ we have $az_3^2 + bz_6 + cz_5 + dz_4 + fz_3 + r \geq a(z_3 + \epsilon y_3)^2 + b(z_6 + \epsilon y_6) + c(z_5 + \epsilon y_5) + d(z_4 + \epsilon y_4) + f(z_3 + \epsilon y_3) + r$, which contradicts the maximality of k . $\square$

Theorem 2.3 (Third degree principle for sextics). *Let $F \in \mathbb{R}[X]^{S_n}$ be a symmetric polynomial of degree 6 that satisfies condition (A).*

- (I) *Let $K = \{x \in \mathbb{R}^n \mid F_1(x) \geq 0, \dots, F_m(x) \geq 0\}$ and $\max\{\deg F_1, \dots, \deg F_m\} = 2$. Then*

$$\inf_{x \in K} = \inf_{x \in K \cap A_2} F(x).$$

- (II) *If F is homogeneous and $n = 3$ then F is psd if and only if $\tilde{F}(X_1, X_2) := F(X_1, X_2, X_2)$ is psd if and only if $\tilde{F}$ is sos.*

Proof. (I) If $K = \mathbb{R}^n$, $\inf_{x \in \mathbb{R}^n} F(x) = \inf_{z \in \mathcal{H}} G(z) = \inf_{(a_1, a_2)} \left(\min_{z \in \mathcal{H}(a_1, a_2)} G(z) \right)$.
 If $K \subsetneq \mathbb{R}^n$, as $\deg F_i \leq 2$ there are G_i such that $F_i(x) = G_i(e_1, e_2)$, $i = 1, \dots, m$.
 Then defining $\tilde{K} := \{(y_1, y_2) \mid G_1(y_1, y_2) \geq 0, \dots, G_m(y_1, y_2) \geq 0\}$,

$$\inf_{x \in K} F(x) = \inf_{(a_1, a_2) \in \tilde{K}} \left(\min_{z \in \mathcal{H}(a_1, a_2)} G(z) \right)$$

In any case, the result follows from proposition 2.2.

(II) A minimizer of F can be found in A_2 , so it is clear that F is psd if and only if $\tilde{F}$ is psd. Finally, $\tilde{F}$ is a homogeneous polynomial in two variables and by Hilbert's theorem is psd if and only if it is sos. $\square$

3. EXAMPLES

Example 3.1. Let $F(x_1, x_2, x_3)$ be the symmetric homogeneous polynomial

$$F = \sum_{i \neq j} x_i^2 x_j^4 + \sum_{i < j} x_i^3 x_j^3 - \sum_{(i, j) \in S_3} x_i x_j^2 x_k^3 + \sum_{i < j, k \neq i, j} x_i x_j x_k^4 - 6x_1^2 x_2^2 x_3^2$$

F satisfies condition (A) since $F(1, e^{2\pi i/3}, e^{-2\pi i/3}) = 0$ (also, it can be checked that $F = e_1^2 e_2^2 - e_1^3 e_3 - e_2^3 - 3e_1 e_2 e_3$). Then $\tilde{F} = 3x_1^4 x_2^2 - 6x_1^2 x_2^2 + 3x_2^6 = 3x_2^2(x_1^2 - x_2^2)^2$ is psd so F is also psd. As an aside issue, it can be shown that F is not sos.

Example 3.2. Let $F(x_1, x_2, x_3)$ be the symmetric polynomial

$$F = x_1^2 x_2^2 x_3^2 + \sum_{i < j} (x_i^2 x_j^2 + 4x_i x_j) + 2 \sum_{i < j, k \neq i, j} x_i x_j x_k^2 + \sum_i x_i^2 + 1$$

It can be checked that F is psd and that all its minimizers $((-1, 0, 1)$ and its permutations) have three distinct coordinates. Of course, F does not verify condition (A), in fact, $F = e_1^2 + (e_2 + 1)^2 + e_3^2$.

REFERENCES

- [1] Hilbert, D. Über die Darstellung definiter Formen als Summe von Formenquadraten. *Math. Ann.* **32** (1888), 342–350.
- [2] Moustrou, P., Riener, C., Verdu, H. Symmetries in polynomial optimization. In *Polynomial Optimization, Moments, and Applications* (2023), 53–111 Springer Nature.
- [3] Riener, C. On the degree and half-degree principle for symmetric polynomials, *J. Pure Appl. Algebra* **216** (2012), 850–866.
- [4] Sturmfels, B. Algorithms in invariant theory. *Texts and Monographs in Symbolic Computation* (2008), Springer.
- [5] Timofte, V. On the positivity of symmetric polynomial functions. I: general results. *J. Math. Anal. Appl.* **284** (2003), 174–190.

Departamento Álgebra, Geometría y Topología, Facultad de Ciencias Matemáticas, Universidad Complutense de Madrid, Spain.

Email address: romue.mira@gmail.com

Instituto de Matemática Interdisciplinar (IMI) - Departamento de Álgebra, Geometría y Topología, Facultad de Ciencias Matemáticas, Universidad Complutense de Madrid, Spain.

Email address: adiazcan@ucm.es

DEFINING EQUATIONS OF POINT CONFIGURATIONS

OLIVER CLARKE, GIACOMO MASIERO, AND FATEMEH MOHAMMADI

ABSTRACT. Point-line configurations give rise to a fundamental class of matroids. We study their associated varieties from the viewpoint of incidence and projective geometry. In particular, we study the irreducible decompositions of these varieties and their defining polynomial equations. Firstly, we focus on specific families of configurations, such as quadrilateral sets and 3×4 grids. Then, we extend our results to less-structured families of configurations, and describe the irreducible decompositions of their matroid varieties.

1. INTRODUCTION

The variety of a matroid is the Zariski closure of its realisation space. This notion, introduced in [6], gives rise to a deep combinatorial structure on the matroid stratification of the Grassmannian. However, understanding properties about these strata, such as their defining equations [15], is a very difficult problem. So, it is natural to restrict attention to particular classes of matroids. For instance, the matroid varieties of uniform matroids have been extensively studied in commutative algebra, as determinantal varieties [1, 5, 12]. In [3], we use incidence geometry to study matroid varieties associated with point-line configurations. Specifically, we seek general methods to translate the incidence structure of the underlying configuration into a geometrically meaningful minimal generating set of its polynomial ideal. We fully complete this task for the quadrilateral sets and 3×4 grids.

The matroid varieties arising from point-line configurations are a rich and diverse family. For example, the Mnëv-Sturmfels Universality Theorem [8, 11] shows that matroid varieties satisfy Murphy's law in algebraic geometry, i.e., given any singularity of a semi-algebraic set, there is a matroid variety with the same singularity, up to a mild equivalence on singularities. Here, the matroid varieties associated with a point-line configuration can achieve all such singularities. Additionally, the extra structure induced by point-line configurations is mirrored in algebraic statistics [2, 4].

The axiomatic definition of matroids dates back to Whitney [17]. Shortly afterwards, the intimate link between matroids and projective geometry was pointed out by MacLane [10]. While this connection is nowadays classical, the use of projective incidence geometry in the study of matroid varieties is quite recent. It has arisen as a tool for constructing and giving geometric interpretations to non-determinantal generators of ideals of matroid varieties.

Example 1.1. In [2, 15, 16], the authors study the arrangement of 7 points on 3 concurrent lines in the plane, with three points on each line and one intersection point. Here, incidence geometry tells that the projective coordinates of the points must satisfy the three collinearities (degree-3 polynomial conditions) and a degree-6 polynomial, whose vanishing is determined by the concurrency of the three lines.

The third author will present the work.

Definition 1.2. Let M be a rank- r matroid on $[n]$ and $C(M)$ its circuits. Let $R = \mathbf{k}[X]$ be a polynomial ring where $X = (x_{i,j})$ is an $r \times n$ matrix of variables. We define the *circuit ideal* as $I_{C(M)} = \langle [B]_X \mid B \in C(M) \rangle \subseteq R$. The *circuit variety* of M is $V_{C(M)} = V(I_{C(M)}) \subseteq \mathbf{k}^{r \times n}$. Here, $[B]_X$ denotes the minor of the submatrix of X on the columns indexed by B .

Let $r \geq \text{rk}(M)$ be a fixed integer. A *realisation* of M over $\mathbf{k}$ is a matrix $V \in \mathbf{k}^{r \times n}$ such that for any subset $I \subseteq [n]$ we have that $[V]_I$ has full rank if and only if I is an independent set of M . The *realisation space* of a matroid in $\mathbf{k}^{r \times n}$ is $\Gamma_M = \{V \in \mathbf{k}^{r \times n} \mid V \text{ is a realisation of } M\}$. The matroid variety $V_M = \overline{\Gamma_M}$ is the Zariski closure in $\mathbf{k}^{r \times n}$ of the realisation space. We denote by $I_M = I(V_M) \subseteq \mathbf{k}[X]$ the ideal of the matroid variety.

Computing a minimal generating set of I_M via incidence geometry helps to overcome the difficulty of numerical computations. One method to compute minimal generating sets is via Gröbner bases. However, these algorithms have high complexity and, consequently, provide results only for small matroids. In addition, the outputs often consist of long polynomials that cannot be parsed by a human, which gives little geometric intuition.

Example 1.3. By direct computation in *Macaulay2* [7], we know that 14 homogeneous polynomials generate the ideal of the matroid variety associated with a quadrilateral set:

- a. Four have degree 3, and reflect the collinearities of the arrangement,
- b. The rest have degree 6, in 18 variables, and are the sum of ≈ 15 monomials.

Example 1.4. In [13], the authors compute that the associated ideal of the 3×4 grid is generated by 44 homogeneous polynomials, where:

- c. Sixteen of them have degree 3, and reflect the collinearities of the arrangement,
- d. The rest have degree 12, in 36 variables, and are the sum of ≈ 250 monomials.

Our contributions. We study the question of determining when a tuple of collinear points in $\mathbb{P}_{\mathbb{C}}^2$ can be lifted to a non-trivial realisation of a fixed point-line configuration $\mathcal{C}$. When this is possible, we call $\mathcal{C}$ *hyperliftable*; and when this is possible, up to removing a line, then we term $\mathcal{C}$ *quasi-hyperliftable*. We analyse such configurations and provide an irreducible decomposition of their circuit varieties. This is our main theoretical contribution, as well as our main tool for studying our central examples. On the computational side, we answer the liftability problem for quadrilateral sets and 3×4 grids. In this way, we characterise the 6-tuples of collinear points that can be lifted to a quadrilateral set, as well as the 12-tuples of collinear points that can be lifted to a 3×4 grid. In particular, for quadrilateral sets, we provide a new characterisation, which is equivalent to the one in [14].

Point-line configurations. We think of matroids of rank three as incidence structures called *point-line configurations*. We study the realisation space of these matroids via incident geometry. An *abstract point-line configuration* is a triple $(\mathcal{P}, \mathcal{L}, \mathcal{I})$. The elements of $\mathcal{P}$ and $\mathcal{L}$ are the *points* and *lines*. Each pair $(p, \ell) \in \mathcal{I} \subseteq \mathcal{P} \times \mathcal{L}$ is an *incidence* and we say that p *lies on* ℓ or ℓ *is incident to* p . An abstract point-line configuration is *linear* if: there is at most one line incident to any pair of points; and every line is incident to at least two points.

Definition 1.5. Let M be a rank-3 matroid. We define the *point-line configuration* $\mathcal{C}_M := ([n], \mathcal{L}_M, \mathcal{I}_M)$ as follows. The point set of $\mathcal{C}_M$ is the ground set $[n]$ of M . The lines $\mathcal{L}_M := \{F \in F(M) \mid \text{rk}(F) = 2, |F| \geq 3\}$ are the rank-two flats of M of size ≥ 3 . The incidences $\mathcal{I}_M$ are given by inclusion, i.e., $(p, \ell) \in \mathcal{I}_M$ if and only if $p \in \ell$.

Point-line arrangements of realisable matroids are typically not linear. The obstructions are *loops* (elements contained in no basis) and non-trivial *parallel classes* (rank-one flats with more than an element). To talk about linear point-line configurations of matroids, we assume them to be *simple*, i.e., loopless and each parallel class a singleton.

Proposition 1.6. *Let M be a simple matroid on $[n]$. Then the point-line configuration $\mathcal{C}_M$ is linear. Particularly, if M has a realisation $A \in \mathbb{C}^{3 \times n}$, then the columns of A are distinct points in $\mathbb{P}_{\mathbb{C}}^2$ and the lines of $\mathcal{C}_M$ correspond to 1-dimensional linear subspaces in $\mathbb{P}_{\mathbb{C}}^2$.*

2. ON LIFTABILITY PROPERTIES OF POINT-LINE CONFIGURATIONS

We first introduce the notion of *(quasi-)hyperliftability* of point-line configurations $\mathcal{C}$.

Definition 2.1. A linear configuration $\mathcal{C}$ with n points is called *hyperliftable* over a field $\mathbf{k}$ if any n -tuple of collinear points in $\mathbb{P}_{\mathbf{k}}^2$ is the projective image of a non-degenerate realisation of $\mathcal{C}$, and $\mathcal{C}$ is *quasi-hyperliftable* if it is not hyperliftable, but $\mathcal{C} \setminus \ell$ is hyperliftable for all ℓ .

We introduce an algebraic tool that plays a crucial role in the liftability problem. Particularly, it gives insights about whether $\mathcal{C}$ is (quasi-)hyperliftable and the conditions that n collinear points must satisfy so that they may be lifted to a non-degenerate realisation of $\mathcal{C}$.

Construction 2.2. Let $\mathcal{C} = (\mathcal{P}, \mathcal{L}, \mathcal{I})$ be a point-line configuration and $\mathbf{k}$ a field. Consider an n -tuple of collinear points $P_1, \dots, P_n$ in $\mathbb{P}_{\mathbf{k}}^2$, where $n = \#\mathcal{P}$. Let $P \in \mathbb{P}_{\mathbf{k}}^2$ be a point that is not collinear with $P_1, \dots, P_n$. After a change of coordinates, we may assume that $P = (0, 0, 1)$ and $P_1 = (x_1, 1, 0), \dots, P_n = (x_n, 1, 0)$ for some $x_i \in \mathbf{k}$, i.e., the points lie on the line $z = 0$. The problem is to find $z_1, \dots, z_n \in \mathbf{k}$ such that the points $(x_i, 1, z_i)$ are a non-degenerate realisation of $\mathcal{C}$. We denote by $[P_i P_j]$ the 2×2 minor $x_i - x_j$. We construct the matrix Λ that encodes all the collinearity conditions imposed by $\mathcal{C}$. The matrix Λ has one column for each point P_i , and one row for each collinearity condition of $\mathcal{C}$, i.e., each triplet of collinear points. Finally, if $\Lambda_{i,-}$ is the row of Λ corresponding to the collinearity condition on $P_{i_1}, P_{i_2}, P_{i_3}$, with $i_1 < i_2 < i_3$ then

$$\Lambda_{i,i_1} = [P_{i_2} P_{i_3}], \quad \Lambda_{i,i_2} = -[P_{i_1} P_{i_3}], \quad \Lambda_{i,i_3} = [P_{i_1} P_{i_2}], \quad \text{and} \quad \Lambda_{i,j} = 0 \quad \text{otherwise.}$$

Suppose that $\ell \subseteq \mathcal{P}$ is a set of collinear points with $\#\ell > 3$. For each 3-subset of ℓ , the above construction gives a row of Λ . These rows are linearly dependent. Moreover, it is straightforward to show that the set of such rows has rank $\#\ell - 2$.

We call Λ the *collinearity matrix* of $\mathcal{C}$. It naturally defines the linear system $\Lambda(z_1 \dots z_n)^t = (0 \dots 0)^t$. If $\mathcal{C}$ is connected then the liftability problem for $\mathcal{C}$ has non-degenerate solutions if and only if the solution space of the system above has dimension ≥ 3 . By this, we mean that there are lifts where not all points are collinear. Note that such solutions may not be a realisation of $\mathcal{C}$ as the lift may contain additional dependencies. See also [9].

Lemma 2.3. *Let M be a realisable simple rank-3 matroid on $[n]$, which is maximal among the realisable simple rank-3 matroids over $[n]$, with respect to the dependency order. Then, the following statements are equivalent, for its point-line configuration $\mathcal{C}_M$.*

- (i) *The configuration $\mathcal{C}_M$ is hyperliftable.*
- (ii) *The linear system $\Lambda(z_1 \dots z_n)^t = 0$, where Λ is the collinearity matrix of $\mathcal{C}_M$, has solution space of dimension at least 3.*

Theorem 2.4. *Assume that $\mathcal{C}_M$ has no triplets of concurrent lines.*

- (i) *If $\mathcal{C}_M$ is hyperliftable then $V_{\mathcal{C}(M)} = V_M$ and $\sqrt{I_{\mathcal{C}(M)}} = I_M$.*
- (ii) *If $\mathcal{C}_M$ is connected and quasi-hyperliftable then $V_{\mathcal{C}(M)} = V_0 \cup V_M$ and $\sqrt{I_{\mathcal{C}(M)}} = I_0 \cap I_M$, where $V_0 = V(I_0)$ is the matroid variety of a line with n points.*

For each item above, the decompositions are irreducible and prime, respectively.

Applying Lemma 2.3, quadrilateral sets and 3×4 grids are quasi-hyperliftable. Utilizing this property, in [3], we compute their ideals, as in Examples 1.3 and 1.4.

REFERENCES

- [1] W. Bruns and A. Conca. Gröbner bases and determinantal ideals. In *Commutative Algebra, Singularities and Computer Algebra*, pages 9–66. Springer Netherlands, 2003.
- [2] O. Clarke, K. Grace, F. Mohammadi, and H. J. Motwani. Matroid stratifications of hypergraph varieties, their realization spaces, and discrete conditional independence models. *International Mathematics Research Notices*, 2023(22):18958–19019, 2023.
- [3] O. Clarke, G. Masiero, and F. Mohammadi. Liftable point-line configurations: Defining equations and irreducibility of associated matroid and circuit varieties. *arXiv preprint arXiv:2402.07737*, 2024.
- [4] O. Clarke, F. Mohammadi, and H. J. Motwani. Conditional probabilities via line arrangements and point configurations. *Linear and Multilinear Algebra*, 70(20):5268–5300, 2022.
- [5] V. Ene, J. Herzog, T. Hibi, and F. Mohammadi. Determinantal facet ideals. *The Michigan Mathematical Journal*, 62(1):39–57, 2013.
- [6] I. M. Gelfand, R. M. Goresky, R. D. MacPherson, and V. V. Serganova. Combinatorial geometries, convex polyhedra, and Schubert cells. *Advances in Mathematics*, 63(3):301–316, 1987.
- [7] M. Grayson, D. R. and Stillman. Macaulay2, a software system for research in algebraic geometry.
- [8] S. H. Lee and R. Vakil. Mnëv-sturm-fels universality for schemes. *A celebration of algebraic geometry*, 18:457–468, 2013.
- [9] E. Liwski and F. Mohammadi. Paving matroids: Defining equations and associated varieties. *arXiv preprint arXiv:2403.13718*, 2024.
- [10] S. MacLane. Some interpretations of abstract linear dependence in terms of projective geometry. *American Journal of Mathematics*, 58(1):236–240, 1936.
- [11] N. E. Mnëv. The universality theorems on the classification problem of configuration varieties and convex polytopes varieties. In *Topology and geometry—Rohlin seminar*, pages 527–543. Springer, 2006.
- [12] F. Mohammadi and J. Rauh. Prime splittings of determinantal ideals. *Communications in Algebra*, 46(5):2278–2296, 2018.
- [13] G. Pfister and A. Steenpass. On the primary decomposition of some determinantal hyperedge ideal. *Journal of Symbolic Computation*, 103:14–21, 2021.
- [14] J. Richter-Gebert. *Perspectives on projective geometry*. Springer, 2011.
- [15] J. Sidman, W. Traves, and A. Wheeler. Geometric equations for matroid varieties. *Journal of Combinatorial Theory, Series A*, 178:105360, 2021.
- [16] B. Sturmfels. Computational algebraic geometry of projective configurations. *Journal of symbolic computation*, 11(5-6):595–618, 1991.
- [17] H. Whitney. On the abstract properties of linear dependence. *Hassler Whitney Collected Papers*, pages 147–171, 1992.

School of Mathematics, University of Edinburgh, Edinburgh, UK

Email address: `oliver.clarke@ed.ac.uk`

Department of Mathematics, KU Leuven, Belgium

Email address: `giacomo.masiero@kuleuven.be`

Department of Mathematics and Computer Science, KU Leuven, Belgium, and Department of Mathematics, The Arctic University of Norway, 9037 Tromsø, Norway

Email address: `fatemeh.mohammadi@kuleuven.be`

PAVING MATROIDS: DEFINING EQUATIONS AND A DECOMPOSITION OF ASSOCIATED VARIETIES

EMILIANO LIWSKI AND FATEMEH MOHAMMADI

ABSTRACT. We study paving matroids, their realization spaces, and their closures, along with matroid varieties. Within this context, we introduce three distinct methods for generating polynomials within the associated ideals of these varieties across any dimension. Additionally, we explain the relationship between polynomials constructed using these different methods. We then compute a comprehensive and finite set of defining equations for matroid varieties associated with specific classes of paving matroids.

1. INTRODUCTION

In this work, we study paving matroids from an algebro-geometric viewpoint. An n -paving matroid M is a matroid in which every circuit has a size equal to either n or $n + 1$, where n represents the rank of M , denoted by $r(M)$. It is conjectured in [13] that asymptotically almost all matroids are paving; see also [12]. Our primary focus lies on the matroid variety V_M , defined as the Zariski closure of the matroid's realization space, which was originally introduced in [9] and has since been extensively studied; see e.g. [3, 4, 17].

The primary question is to find a complete and finite set of defining equations, or equivalently, a finite set of generators of the ideal of the matroid variety $I_M = I(V_M)$ and to represent such polynomials geometrically or combinatorially. Equally significant is the task of determining an irredundant irreducible decomposition of the matroid variety V_M . Notably, it is established that the circuit ideal $I_{C(M)}$, generated by the polynomials associated with the circuits of M , is always a subset of I_M . However, the reverse is rarely true. In the case of a positroid, it was demonstrated in [10] that the two ideals $I_{C(M)}$ and I_M coincide. Additionally, positroid varieties are also irreducible. However, this is not true in most cases; in [20], Sturmfels introduced a minimal example where $I_{C(M)} \subsetneq I_M$ and I_M is reducible. In [17], the authors computed such polynomials in $I_M \setminus I_{C(M)}$ using the Grassmann-Cayley algebra, for specific family of point-line configurations. A classical method for computing such polynomials within the matroid ideal I_M applies the Grassmann-Cayley algebra, which offers a combinatorial approach. However, fully generating all polynomials in I_M , or verifying whether those generated by the Grassmann-Cayley method are sufficient, remains challenging. This challenge arises due to the saturation step included in the matroid ideal's construction, see e.g. [2, 17, 18, 19, 21].

Existing algorithms for computing the saturation of ideals are characterized by high complexity, thereby limiting their practicality to small-scale matroids. Furthermore, the resulting polynomials often lack geometric insight, being lengthy and challenging to interpret. This limitation is illustrated by examples in [4, 15]. Given the complexity associated

The first author will present the work.

with computing the entire ideal, there has been considerable interest in generating certain polynomials, albeit not necessarily the entire generating set, for the ideal I_M , particularly for specific families of matroids. For instance, in [17], the authors applied the Grassmann-Cayley algebra in combination with geometric tools from [2, 7] to generate polynomials for a family of examples of point-line configurations. Another geometric approach, not relying on the Grassmann-Cayley algebra, was applied in [4] for rank-3 matroids, leading to computation of a minimal generating set for the matroid ideals of quadrilateral sets and the 3×4 grid. Our work extends these geometric techniques to matroids of arbitrary ranks.

2. MAIN RESULTS

In general, finding a finite set of generators for I_M can be quite challenging, and they also appear in the context of conditional independence statements [1, 5, 6, 8, 14].

Question. Consider an n -paving matroid M and let γ be a collection of vectors in $\mathbb{C}^n$ indexed by the elements of M , lying within a hyperplane H of $\mathbb{C}^n$, with $q \in \mathbb{C}^n \setminus H$. What condition is both necessary and sufficient for the existence of a lifting of the vectors from γ at point q to a non-degenerate collection $\tilde{\gamma} \in V_{C(M)}$?

We address this question in [11], where we establish that the desired lifting exists if and only if certain minors of a so-called liftability matrix vanish on the vectors of γ . More precisely, for any vector $q \in \mathbb{C}^n$ and any n -paving matroid M , we define the *liftability matrix* $\mathcal{M}_q(M)$ with columns indexed by the elements of M and rows indexed by the n -circuits of M . For each n -circuit $c = \{c_1, c_2, \dots, c_n\}$, the c_i^{th} coordinate of the corresponding row is given by the polynomial $(-1)^{i-1} [c_1, c_2, \dots, c_{i-1}, \hat{c}_i, c_{i+1}, \dots, c_n, q]$.

Notably, projecting the vectors from any realization of an n -paving matroid M onto a hyperplane in $\mathbb{C}^n$ from a point outside of it ensures that the projected vectors satisfy the condition for non-degenerate lifting to exist. This observation holds true for any submatroid of full rank within M , as well. Using this, we can construct polynomials within I_M .

Theorem 2.1. *Let M be an n -paving matroid and N a submatroid of M of full rank. Then, for any $q \in \mathbb{C}^n$, the $|N| - n + 1$ minors of the matrix $\mathcal{M}_q(N)$ are polynomials within I_M .*

Such polynomials are called *lifting polynomials*, and I_M^{lift} denotes the ideal they generate.

Theorem 2.2. *Let M be an n -paving matroid with no points of degree greater than two. Then, the circuit and lifting polynomials generate the matroid ideal, up to radical, as follows:*

$$I_M = \sqrt{I_{C(M)} + I_M^{\text{lift}}}.$$

Applying the above theorem, which provides a comprehensive description of the defining equations of the matroid varieties of this type, we can compare the matroid variety and the circuit variety of M . Below, we use the notation $V_{C(M)}$ and V_M for the circuit variety and the matroid variety, respectively. We denote V_0 for the variety of the uniform matroid.

Theorem 2.3. *Let M be an n -paving matroid with no points of degree greater than two.*

- *If all submatroids of M are liftable, then $V_{C(M)} = V_M$.*
- *If all proper submatroids of M are liftable, then $V_{C(M)} = V_M \cup V_0$.*

In [11, §5], we introduce a combinatorial approach for generating polynomials within I_M . Every such polynomial is uniquely linked to a specific graph. To see this, consider

two subsets of elements of M , J and $P = \{p_1, \dots, p_k\}$, such that $P \cap \bar{J} = \emptyset$. Suppose $C = \{c_1, \dots, c_k\}$ is a set of circuits of size n whose points belong to $J \cup P$, and $p_i \in c_i$ for every i . For any realization $\gamma \in \Gamma_M$, construct a directed weighted graph G on the vertex set P , where the weights are the coefficients of some linear dependencies on the vectors $\{\gamma_p : p \in P\}$ arising from the circuits c_i . We show that such weights satisfy a polynomial relation. Moreover, we illustrate that these weights can be substituted with quotients of polynomial brackets by selecting an additional set of vectors $\{q_p : p \in P\} \subset \mathbb{C}^n$. Upon multiplying by the denominators of these quotients, we derive a polynomial involving the brackets that vanishes at γ . Since γ is a realization of M , we obtain a polynomial within I_M . We refer to such polynomials as *graph polynomials*, which generate the ideal I_M^{graph} .

Theorem 2.4. *Let M be an n -paving matroid with no points of degree greater than two. Then I_M^{graph} contains the ideal I_M^{lift} , and the circuit polynomials and graph polynomials together form a finite generating set for the matroid ideal, up to radical: $I_M = \sqrt{I_{C(M)} + I_M^{\text{graph}}}$.*

3. RELATED WORKS

We now comment on some related works. In [20], Sturmfels introduced the concept of projection, focusing specifically on the quadrilateral set. He provided an explicit polynomial condition for the liftability of six collinear points to a quadrilateral set and algorithmically derived their standard bracket representation. In [16], Richter applied a similar projection technique to characterize the liftability of six points on a line to a quadrilateral set using determinant equations involving the center of projection. A generalization of this liftability technique was also presented in [4] for 3-rank matroids and was applied to explicitly compute a minimal generating set for the associated ideals of the quadrilateral sets and the matroid of the 3×4 grid. In our work, we extend this technique to any paving matroid of any dimension by projecting onto a hyperplane instead of a line. In [3], it was established that forest-type point-line configurations are realizable. We show that n -paving matroids with no points of degree greater than two are also realizable. This expansion broadens the scope of known realizable matroids. We also note that the polynomials constructed using our methods differ from those constructed using the Grassmann-Cayley algebra. For example, concerning the Pascal matroid studied in [17], our main result illustrates that the polynomials constructed in Theorem 2.2 are not contained in the ideal generated by the polynomials constructed in [17] using the Grassmann-Cayley algebra. Additionally, in [17, Theorem 4.2.2], the authors constructed a matroid from $d + 4$ points on a rational normal curve of degree d via the Grassmann-Cayley algebra. Applying Theorem 5.1 of [2], they demonstrated the existence of non-trivial quartics in the associated matroid ideal using the Grassmann-Cayley algebra.

REFERENCES

- [1] P. Caines, F. Mohammadi, E. Sáenz-de Cabezón, and H. Wynn. Lattice conditional independence models and Hibi ideals. *Transactions of the London Mathematical Society*, 9(1):1–19, 2022.
- [2] A. Caminata and L. Schaffler. A Pascal’s theorem for rational normal curves. *Bulletin of the London Mathematical Society*, 53(5):1470–1485, 2021.
- [3] O. Clarke, K. Grace, F. Mohammadi, and H. Motwani. Matroid stratifications of hypergraph varieties, their realization spaces, and discrete conditional independence models. *International Mathematics Research Notices*, page rnac268, 2022.

- [4] O. Clarke, G. Masiero, and F. Mohammadi. Lifiable point-line configurations: defining equations and irreducibility of associated matroid and circuit varieties. *arXiv preprint arXiv:2402.07737*, 2024.
- [5] O. Clarke, F. Mohammadi, and H. Motwani. Conditional probabilities via line arrangements and point configurations. *Linear and Multilinear Algebra*, 70(20):5268–5300, 2022.
- [6] O. Clarke, F. Mohammadi, and J. Rauh. Conditional independence ideals with hidden variables. *Advances in Applied Mathematics*, 117:102029, 2020.
- [7] D. Eisenbud, M. Green, and J. Harris. Cayley-Bacharach theorems and conjectures. *Bulletin of the American Mathematical Society*, 33(3):295–324, 1996.
- [8] V. Ene, J. Herzog, T. Hibi, and F. Mohammadi. Determinantal facet ideals. *Michigan Mathematical Journal*, 62(1):39–57, 2013.
- [9] I. Gelfand, M. Goresky, R. MacPherson, and V. Serganova. Combinatorial geometries, convex polyhedra, and Schubert cells. *Advances in Mathematics*, 63(3):301–316, 1987.
- [10] A. Knutson, T. Lam, and D. E. Speyer. Positroid varieties: juggling and geometry. *Compositio Mathematica*, 149(10):1710–1752, 2013.
- [11] E. Liwski and F. Mohammadi. Paving matroids: Defining equations and associated varieties. *arXiv preprint arXiv:2403.13718*, 2024.
- [12] L. Lowrance, J. Oxley, C. Semple, and D. Welsh. On properties of almost all matroids. *Advances in Applied Mathematics*, 50(1):115–124, 2013.
- [13] D. Mayhew, M. Newman, D. Welsh, and G. Whittle. On the asymptotic proportion of connected matroids. *European Journal of Combinatorics*, 32(6):882–890, 2011.
- [14] F. Mohammadi and J. Rauh. Prime splittings of determinantal ideals. *Communications in Algebra*, 46(5):2278–2296, 2018.
- [15] G. Pfister and A. Steenpass. On the primary decomposition of some determinantal hyperedge ideal. *Journal of Symbolic Computation*, 103:14–21, 2019.
- [16] J. Richter-Gebert. *Perspectives on Projective Geometry: A Guided Tour Through Real and Complex Geometry*. Springer Berlin Heidelberg, 2011.
- [17] J. Sidman, W. Traves, and A. Wheeler. Geometric equations for matroid varieties. *Journal of Combinatorial Theory, Series A*, 178:105360, 2021.
- [18] M. Sitharam, A. S. J., and J. Sidman. *Handbook of Geometric Constraint Systems Principles (1st edition)*. Chapman and Hall/CRC, Boca Raton, 2017.
- [19] B. Sturmfels. On the matroid stratification of Grassmann varieties, specialization of coordinates, a problem of N. White. *Advances in Mathematics*, 75(2):202–211, 1989.
- [20] B. Sturmfels. *Algorithms in invariant theory*. Texts and Monographs in Symbolic Computation, Springer-Verlag, Vienna, 1993.
- [21] N. L. White. Geometric applications of the Grassmann-Cayley algebra. In *Handbook of discrete and computational geometry*, pages 1581–1592. Chapman and Hall/CRC, 2017.

Department of Mathematics, KU Leuven, Belgium
 Email address: `emiliano.liwski@kuleuven.be`

Department of Mathematics, KU Leuven, Belgium
 Email address: `fateme.h.mohammadi@kuleuven.be`

SUPPORT OF THE MINIMAL POLYNOMIAL IN THE DIFFERENTIAL DYNAMICAL SYSTEM

YULIA MUKHINA AND GLEB POGUDIN

ABSTRACT. Differential elimination refers to finding consequences of a system of differential equations depending only on a chosen subset of variables. In the context of dynamical modeling, one often starts with a polynomial dynamical system of the form $\mathbf{x}' = \mathbf{g}(\mathbf{x})$ and is interested to obtain the minimal equation satisfied by a single component of $\mathbf{x}$ (for example, x_1). Based on the degrees of the polynomials in $\mathbf{g}$, we give an upper bound on the support of such minimal equation which can be further used, for example, for computing this equations using an ansatz. We show that our bound is sharp in the planar case.

INTRODUCTION

Differential elimination is a differential analogue of elimination for polynomial systems and Gaussian elimination from linear algebra. Its study has been initiated by Ritt [6], the founder of differential algebra, in the 1930s. He developed the foundations of the characteristic set approach, which has been made fully constructive by Seidenberg [7]. The algorithmic aspect of this research culminated in the Rosenfeld-Gröbner algorithm [1, 4] implemented in the BLAD library [2] (available through Maple). We will focus on a special case of differential elimination of practical importance, namely, given a system of polynomial ordinary differential equations (ODEs)

$$(1) \quad \mathbf{x}' = \mathbf{g}(\mathbf{x}),$$

compute an equation of the minimal order satisfied by x_1 -component of every solution of (1). This question naturally arises, for example, if experimental data is not available for other variables [3].

1. PRELIMINARIES

In order to state the main problem more precisely, we fix a field $\mathbb{K}$ of characteristic zero. For a set of variables $\mathbf{x} = (x_1, \dots, x_n)$, one can define a *ring of differential polynomial in $\mathbf{x}$* as a ring of infinitely many variables in $\mathbf{x}$ and its formal derivatives:

$$R = \mathbb{K}[\mathbf{x}^{(\infty)}] = \mathbb{K}[x_i^{(j)} \mid 1 \leq i \leq n, 0 \leq j].$$

This ring can be endowed with a structure of a differential ring by defining a derivation $'$ to be zero on $\mathbb{K}$ and $(x_i^{(j)})' = x_i^{(j+1)}$ for every $1 \leq i \leq n$ and $0 \leq j$. For a polynomial $p \in \mathbb{K}[\mathbf{x}^{(\infty)}]$ and $1 \leq i \leq n$, we will call the largest j such that $x_i^{(j)}$ appears in p the *order* of p respect to x_i , and if p does not involve x_i , we set the order equal to -1 .

This work has been supported by the French ANR-22-CE48-0008 OCCAM project.
The talk at the meeting EACA 2024 has been given by the first author.

An ideal $I \subset R$ is called a *differential ideal* if $a' \in I$ for every $a \in I$. For any $f_1, \dots, f_s \in R$, we denote by $\langle f_1, \dots, f_s \rangle^{(\infty)}$ the differential ideal

$$\langle f_1^{(\infty)}, \dots, f_s^{(\infty)} \rangle.$$

To a system of polynomial ODEs (1), with $\mathbf{g} \in \mathbb{K}[\mathbf{x}]^n$, one can assign a differential ideal $\langle \mathbf{x}' - \mathbf{g}(\mathbf{x}) \rangle^{(\infty)}$. Then, by the differential Nullstellensatz [5, Proposition 2.4], the equations satisfied by the x_1 -component of every (formal power series) solution of (1) are exactly the elimination ideal

$$\langle \mathbf{x}' - \mathbf{g}(\mathbf{x}) \rangle^{(\infty)} \cap \mathbb{K}[x_1^{(\infty)}].$$

It is known that this ideal is prime [5, Proposition 1.24] and that it is completely defined by its minimal polynomial [5, Proposition 1.15] (polynomials are first ordered by the order and then by the total degree) which we will denote by $f_{\min}$.

2. MAIN RESULTS

Theorem 2.1. *Let $g_1, \dots, g_n$ be polynomials in $\mathbb{K}[x_1, \dots, x_n] = \mathbb{K}[\mathbf{x}]$ of degrees $d_1, d_2, \dots, d_n$ such that $D := \max_{2 \leq i \leq n} d_i > 0$ and $d_1 > 0$, and let $I = \langle \mathbf{x}' - \mathbf{g} \rangle^{(\infty)}$. Let $f_{\min} \in \mathbb{K}[x_1^{(\infty)}]$ be the minimal polynomial of $I \cap \mathbb{K}[x_1^{(\infty)}]$ and $\text{ord } f_{\min} \leq \nu$ ($\nu = n$ can be always used).*

Then for every monomial $x_1^{s_0}(x_1')^{s_1} \dots (x_1^{(\nu)})^{s_\nu}$ in $f_{\min}$ the following inequalities hold

(1) *if $d_1 \leq D$*

$$s_0 + \sum_{k=1}^{\nu} (d_1 + (k-1)(D-1))s_k \leq \prod_{k=1}^{\nu} (d_1 + (k-1)(D-1));$$

(2) *if $d_1 > D$, for every $0 \leq \ell < \nu$, we have*

$$\begin{aligned} & \sum_{k=0}^{\ell} (k(D-1) + 1)s_k + \sum_{i=1}^{\nu-\ell} (i(d_1-1) + \ell(D-1) + 1)s_{i+\ell} \leq \\ & \leq \prod_{k=1}^{\ell} (d_1 + (k-1)(D-1)) \prod_{i=1}^{\nu-\ell} (i(d_1-1) + \ell(D-1) + 1). \end{aligned}$$

The inequalities given in the theorem below are the specializations of the ones from Theorem 2.1, and we claim that they defined exactly the Newton polytope for a generic planar ODE system. To state this precisely, let us denote, for any $d \in \mathbb{Z}_{\geq 0}$, by V_d the space of all polynomials in $\mathbb{K}[x_1, x_2]$ of degree at most d .

Theorem 2.2 (Generic sharpness in the planar case). *Let $(d_1, d_2) \in (\mathbb{Z}_{>0})^2$. Then there exist a nonempty Zariski open subset $U \subset V_{d_1} \times V_{d_2}$ such that, for every pair of polynomials $(g_1, g_2) \in U$, the Newton polytope of the minimal polynomial $f_{\min}$ of the differential ideal $I \cap \mathbb{K}[x_1^{(\infty)}]$, where $I = \langle x_1' - g_1(x_1, x_2), x_2' - g_2(x_1, x_2) \rangle^{(\infty)}$, can be described as follows. For monomials $x_1^{s_0}(x_1')^{s_1}(x_1'')^{s_2}$ in $f_{\min}$ the following inequalities hold*

(1) *if $d_1 \leq d_2$*

$$s_0 + d_1 s_1 + (d_1 + d_2 - 1)s_2 \leq d_1(d_1 + d_2 - 1);$$

(2) if $d_1 > d_2$

$$\begin{aligned} s_0 + d_1 s_1 + (2d_1 - 1)s_2 &\leq d_1(2d_1 - 1), \\ s_0 + d_2 s_1 + (d_1 + d_2 - 1)s_2 &\leq d_1(d_1 + d_2 - 1); \end{aligned}$$

Remark 2.3. The polytopes described in Theorem 2.2 can be described and visualized as follows.

(1) **For $d_1 \leq d_2$:** a tetrahedron (see Figure 1a) with vertices

$$(0, 0, 0), (d_1(d_1 + d_2 - 1), 0, 0), (0, d_1 + d_2 - 1, 0), (0, 0, d_1).$$

(2) **For $d_1 > d_2$:** a pyramid (see Figure 1b) with vertices

$$(0, 0, 0), (d_1(d_1 + d_2 - 1), 0, 0), (d_1(d_1 - 1), d_1, 0), (0, 2d_1 - 1, 0), (0, 0, d_1).$$

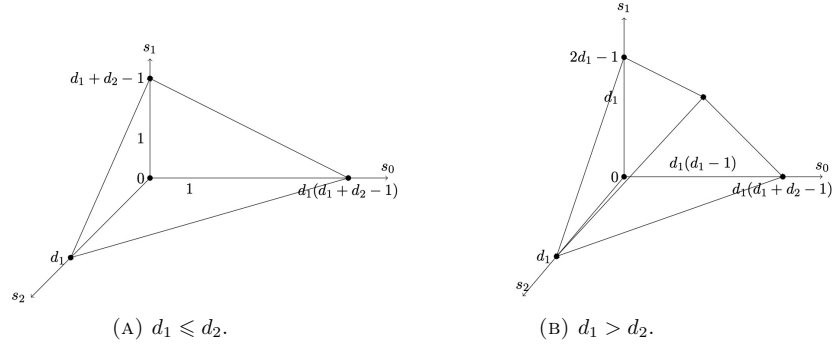


FIGURE 1. Newton polytope of the minimal polynomial in the $n = 2$ case

REFERENCES

- [1] Boulier F., Lazard D., Ollivier F., Petitot M. *Computing representations for radicals of finitely generated differential ideals*. *Applicable Algebra in Engineering, Communication and Computing*, **20** (2009), pp. 73–121.
- [2] Boulier F. *BLAD*. Bibliothèques Lilloises d'Algèbre Différentielle. URL: <https://pro.univ-lille.fr/francois-boulier/logiciels/blad/>
- [3] Dong R., Goodbrake C., Harrington H.A., Pogudin G. *Differential elimination for dynamical models via projections with applications to structural identifiability*. *SIAM Journal on Applied Algebra and Geometry*, **7** (2023), issue 1.
- [4] Hubert E. *Notes on triangular sets and triangulation-decomposition algorithms II: Differential systems*. *Lecture Notes in Computer Science*. Springer Berlin Heidelberg, (2003), 40–87.
- [5] Pogudin G. *Lecture notes on differential algebra*. URL: http://www.lix.polytechnique.fr/Labo/Gleb.POGUDIN/files/da_notes.pdf. 2020.
- [6] Ritt J.F. *Differential Equations from the Algebraic Standpoint*. *Colloquium Publications*. American Mathematical Society, Providence, 1932.
- [7] Seidenberg A. *An elimination theory for differential algebra*. *University of California publications in Mathematics*, **3** (1956), pp. 31–66.

LIX, CNRS, École Polytechnique, Institute Polytechnique de Paris, France
Email address: `gleb.pogudin@polytechnique.edu`

LIX, CNRS, École Polytechnique, Institute Polytechnique de Paris, France
Email address: `yulia.mukhina@lix.polytechnique.fr`

COMPUTATIONAL APPROACH IN THE STUDY OF THE RIGIDITY OF REAL LIE ALGEBRAS.

FRANCISCO OVIAÑO GARCÍA AND RUTWIG CAMPOAMOR STURSBURG

ABSTRACT. In the study of the rigidity of Lie algebras, the cohomological approach has proven to be very useful for determining the rigidity of certain algebras. To this end, a code has been developed for the Mathematica[®] symbolic computation package that allows the calculation of the second Chevalley cohomology space of the real solvable Lie algebras of rank one. This code uses the Hochschild-Serre spectral sequence, being effective for computations in high dimensions.

INTRODUCTION

The study of the rigidity of Lie algebras, which is in principle a topological notion, admits a purely algebraic approach, due to the Nijenhuis-Richardson criterion, that shows that a Lie algebra with zero second Chevalley cohomology space is rigid. Although this criterion is not sufficient, as there are rigid Lie algebras with non-zero cohomology, it allows us to establish the rigidity of a wide range of algebras. This approach allows a computational treatment of the problem.

An obstruction to the calculation of the second group of cohomology is the high number of variables that appear in the calculation of the 2-cochains when the dimension of the algebra is greater than ten, a fact that makes difficult the effective calculation, from a computational point of view. However, making use of the Hochschild-Serre spectral sequence, the necessary memory and computation time used is considerably reduced. In this context, a specific code for the symbolic calculation package Mathematica[®] has been developed, allowing a systematical search of cohomologically rigid (solvable) Lie algebras (of rank one).

Definition 1. A Lie algebra $\mathfrak{g}$ is called rigid if $\mathcal{O}(\mathfrak{g})$ is an open set of $\mathcal{L}^n$ with respect to the Euclidean topology.

Proposition 1. *If the Lie algebra $\mathfrak{g}$ satisfies $\dim H^2(\mathfrak{g}, \mathfrak{g}) = 0$, then it is rigid [9].*

The main tool for practical computations is the Hochschild-Serre factorization theorem [7]. We focus on solvable Lie algebras given by the semi-direct sum $\mathfrak{r} = \mathfrak{t} \overrightarrow{\oplus} \mathfrak{n}$, where $\mathfrak{t}$ is an external torus of derivations that acts diagonally on $\mathfrak{n}$. Under these assumptions, the spaces $H^s(\mathfrak{r}, \mathfrak{r})$ are determined by the relation

$$(1) \quad H^s(\mathfrak{r}, \mathfrak{r}) \simeq \sum_{p+q=s} H^p(\mathfrak{t}, \mathbb{R}) \otimes H^q(\mathfrak{n}, \mathfrak{r})^{\mathfrak{t}},$$

Date: 13/03/2024.

The talk at the meeting EACA 2024 has been given by the Francisco Oviaño García.

with $H^q(\mathfrak{n}, \mathfrak{r})^{\mathfrak{t}}$ the space formed by all $\mathfrak{t}$ -invariant cocycle classes of $\mathfrak{n}$ with values in $\mathfrak{r}$:

$$(2) \quad H^s(\mathfrak{n}, \mathfrak{r})^{\mathfrak{t}} = \{[\varphi] \in H^s(\mathfrak{n}, \mathfrak{r}) \mid (T \cdot \varphi) = 0, \forall T \in \mathfrak{t}\}.$$

The $\mathfrak{t}$ -invariance of a cocycle φ is defined as

$$(3) \quad (T \cdot \varphi)(Z_1, \dots, Z_b) = [T, \varphi(Z_1, \dots, Z_b)] - \sum_{s=1}^b \varphi(Z_1, \dots, [T, Z_s], \dots, Z_b).$$

1. JACOBI CONDITIONS. ALGORITHM FOR FINDING COHOMOLOGICALLY RIGID ALGEBRAS WITH FIXED EIGENVALUE SPECTRUM

The first step of the procedure is to determine the nilradicals that admit a given torus of derivations. We illustrate the procedure with a specific case. Let $\mathfrak{g} = \mathfrak{t} \oplus \mathfrak{n}$ be a solvable Lie algebra with n -dimensional filiform nilradical $\mathfrak{n} = \mathbb{R}\langle X_1, X_2, \dots, X_n \rangle$ and eigenvalue spectrum $\text{spec}(\mathfrak{t}) = \{1, k, k+1, \dots, n+k-2\}$. The only possible brackets are

$$(4) \quad [X_1, X_j] = C_{1,j}^{j+1} X_{j+1}, \quad [X_i, X_j] = C_{i,j}^{i+j+k-2} X_{i+j+k-2}, \quad (2 \leq i < j; i+j+k-2 \leq n).$$

The assumption on the characteristic sequence implies that $C_{1,j}^{j+1} \neq 0$ holds for any j , so that by a change of basis we can set $C_{1,j}^{j+1} = 1$ for $j = 2, \dots, n-1$. The Jacobi identity for $\{X_1, X_i, X_j\}$ provides a first generic relation for $C_{i,j}^l$ in $\mathfrak{n}$:

$$(5) \quad C_{i,j}^{i+j+k-2} - C_{i+1,j}^{i+j+k-1} - C_{i,j+1}^{i+j+k-1} = 0, \quad 2 \leq i < j \leq n-2.$$

These equations determine a linear system that can be solved recursively for the coefficients $C_{i,j}^{i+j+k-2}$ with $|j-i| > 1$ with respect to the set of diagonal entries

$$(6) \quad \Delta = \{\alpha_2, \dots, \alpha_\rho\} = \left\{ C_{2,3}^{k+3}, C_{3,4}^{k+5}, \dots, C_{\rho,\rho+1}^{2\rho+k-1} \right\}, \quad \rho = \left\lfloor \frac{n+1-k}{2} \right\rfloor,$$

leading to the commutators $[X_i, X_{i+1}] = \alpha_i X_{2i+k-1}$, $(2 \leq i \leq \rho)$ and $[X_i, X_{i+s}] = \sum_{\ell=2}^{\rho} \lambda_{i,s}^{\ell} \alpha_{\ell} X_{2i+k+s-2}$ ($i \geq 2$, $2i+k+s-2 \leq n$). Admissible Lie algebras are obtained as solutions of the quadratic system

$$(7) \quad \mathcal{S}: C_{i,j+\ell+k-2}^{i+j+2k+\ell-4} C_{j,\ell}^{j+\ell+k-2} + C_{i,j}^{i+j+k-2} C_{\ell,i+j+k-2}^{i+j+\ell+2k-4} + C_{i,\ell}^{i+\ell+k-2} C_{j,i+\ell+k-2}^{i+j+\ell+2k-4} = 0,$$

reducible to a quadratic system with respect to the variables $\{\alpha_2, \dots, \alpha_\rho\}$ of Δ . An algorithmic procedure to find the (cohomologically rigid) solutions of Lie algebras of (7) for fixed values of n and k can be formulated as follows:

- (1) Start with $q = \rho - 1$.
- (2) In the main diagonal Δ , set $\alpha_{q+1} = 1$ and $\alpha_{\ell} = 0$ for $2 \leq \ell \leq q$.
- (3) If the linear equations (5) are incompatible, then replace q by $q-1$ and go to step 3.
- (4) If (5) is satisfied, evaluate the system $\mathcal{S}$ formed by the Jacobi identities for the generators $\{X_i, X_j, X_{\ell}\}$ with $2 \leq i < j < \ell$.
- (5) If the system $\mathcal{S}$ admits no solution, then replace q by $q-1$ and go to step 3.
- (6) If the system $\mathcal{S}$ admits a solution depending on one or more parameters α_i , then replace q by $q-1$ and go to step 3.

- (7) If the system S admits an isolated solution, take n as the corresponding nilpotent Lie algebra.
- (8) Compute $H^2(\vec{t} \oplus n, \vec{t} \oplus n)$.

Special types of solutions can further be obtained imposing some constraints on Δ , such as the nullity of one or more entries. In these cases however, an additional step (7') has to be introduced, in order to verify that the resulting algebra does not admit supplementary external derivations.

2. CODE FOR THE COHOMOLOGY COMPUTATION

Once the isolated solutions of the Jacobi conditions have been determined, the cohomology is computed using the Hochschild-Serre spectral sequence [11]. The input data are the coefficient matrix and the eigenvalue spectrum of the torus t .

Definition of 1-coboundary invariants and their properties

CB[$X[i_]$]:=If[$i \leq NN$, $z[i, i]X[i]$, 0] **COB** = **Flatten**[**Table**[**CB**[$X[i]$], { i , 1, NN }]]
CAR = **Table**[$z[i, i]$, { i , 1, NN }]

Coboundary relations:

B3[$i_$, $j_$]:= $K[X[i], CB[X[j]]] - K[X[j], CB[X[i]]] - CB[K[X[i], X[j]]]$
CB[$a_X_$]:= $aCB[X]$; **CB**[0]:=0;
CB[$K[X_ + Y_]$, $Z_$]:= $CB[K[X, Z]] + CB[K[Y, Z]]$;
 $K[CB[X_ + Y_]$, $W_$]:= $K[CB[X], W] + K[CB[Y], W]$;
 $K[W_]$, $CB[X_ + Y_]$:= $K[W, CB[X]] + K[W, CB[Y]]$; **CB**[$T[l_]$] = 0;

Table of the 2-coboundary t -invariants:

C3T = **Table**[**B3**[i, j], { i , 1, NN }, { j , 1, NN }]
C3T1 = **DeleteCases**[**Flatten**[**C3T**], 0]/. $X[i_]$ $\rightarrow$ 1
SOO = **Flatten**[**Solve**[**C3T** == 0, **CAR**]] **JJJ** = **CAR**/. **SOO**
SO3 = **Solve**[**JJJ** = 0]
POL = **Solve**[**LOL** = 0, **CAR**]
UIP = **Flatten**[**Keys**[**POL**]]
Length[**UIP**]

Invariant 2-cochains. General relations:

$\Psi[X_ + Y_]$, $Z_$:= $\Psi[X, Z] + \Psi[Y, Z]$
 $\Psi[X_]$, $Y_ + Z_$:= $\Psi[X, Y] + \Psi[X, Z]$
 $\Psi[K[X_ + Y_]$, $Z_]$:= $\Psi[K[X, Z], W] + \Psi[K[Y, Z], W]$
 $\Psi[W_]$, $K[X_ + Y_]$, $Z_$:= $\Psi[W, K[X, Z]] + \Psi[W, K[Y, Z]]$
 $K[\Psi[X_ + Y_]$, $Z_]$:= $K[\Psi[X, Z], W] + K[\Psi[Y, Z], W]$
 $K[W_]$, $\Psi[X_ + Y_]$, $Z_$:= $K[W, \Psi[X, Z]] + K[W, \Psi[Y, Z]]$
 $\Psi[T[l_]$, $X[i_]$:=0, $\Psi[X[i_]$, $T[l_]$:=0, $\Psi[X[i_]$, $X[i_]$:=0, $\Psi[0, X[i_]$:=0, $\Psi[X[i_]$, 0]:=0
 $\Psi[a_X_]$, $Z_$:= $a * \Psi[X, Z]$, $\Psi[Z_]$, $a_X_$:= $a * \Psi[Z, X]$, $c[i_]$, $i_$, $j_$ = 0;

Definition of invariants 2-cochains

$c[i_]$, $j_]$, $p_$:=
If[**EW**[i] + **EW**[j] == **EW**[p], **Signature**[{ i, j }] * $q[\text{Sort}[\{i, j\}][[1]], \text{Sort}[\{i, j\}][[2]], p]$, 0]
 $\Psi[X[i_]$, $X[j_]$:= **Sum**[$c[i, j, p]X[p]$, { p , 1, NN }]
DERF[$l_$, $i_]$, $j_$:= $K[T[l], \Psi[X[i], X[j]]] - K[X[i], \Psi[T[l], X[j]]] + K[X[j], \Psi[T[l], X[i]]] -$

```

Ψ[K[T[l], X[i]], X[j]] + Ψ[K[T[l], X[j]], X[i]] - Ψ[K[X[i], X[j]], T[l]]
KOCI = Table[Ψ[X[i], X[j]], {i, 1, NN}, {j, i + 1, NN}];
NCOC = DeleteCases[Flatten[KOCI], 0]/.X[i_] → 1;
DERC[l_, i_, j_] := K[X[l], Ψ[X[i], X[j]]] - K[X[i], Ψ[X[l], X[j]]] + K[X[j], Ψ[X[l], X[i]]] -
Ψ[K[X[l], X[i]], X[j]] + Ψ[K[X[l], X[j]], X[i]] - Ψ[K[X[i], X[j]], X[l]]
SOCO = Table[DERC[i, j, l], {i, 1, NN}, {j, i + 1, NN}, {l, j + 1, NN}];
SOTO = DeleteCases[Flatten[SOCO], 0]/.X[i_] → 1;
LR = Flatten[Solve[SOTO == 0, NCOC]]; SL = KOCI/.LR; KOKO = KOCI/.LR;
PR = Flatten[Solve[SL == 0, NCOC]]; PRR = Keys[PR];
The dimension of the second cohomology group is:
DIH2 = Length[PR] - Length[UIP]

```

REFERENCES

- [1] Bermúdez, J. A.; Campoamor-Stursberg, R.; Oviaño García, F. New examples of rank one solvable real rigid Lie algebras possessing a nonvanishing Chevalley cohomology. *Applied Mathematics and Computation*, **2018**, 339, 431-440.
- [2] Campoamor-Stursberg, R.; Oviaño García, F. Construction of Rank-One Solvable Rigid Lie Algebras with Nilradicals of a Decreasing Nilpotence Index. *Axioms*, **2023** 12, 8, 754.
- [3] Campoamor-Stursberg, R.; Oviaño García, F. Computer-aided analysis of solvable rigid Lie algebras with a given eigenvalue spectrum. *Axioms*, **2022** 11, 9, 442.
- [4] Campoamor-Stursberg, R.; Oviaño García, F. Algorithmic construction of solvable rigid Lie algebras determined by generating functions. *Linear and Multilinear Algebra*, **2022** 70, 2, 280-296.
- [5] Campoamor-Stursberg, R.; Oviaño García, F. (2019). Some features of rank one real solvable cohomologically rigid Lie algebras with a nilradical contracting onto the model filiform Lie algebra $\mathcal{Q}_n$. *Axioms*, **2019** 8, 1, 10.
- [6] Grozman, P.; Leites, D. Mathematica® aided study of Lie algebras and their cohomology. From supergravity to ballbearings and magnetic hydrodynamics. *Trans. Eng. Sci.* **1997**, 15, 185-192.
- [7] G. Hochschild, J. P. Serre. Cohomology of Lie algebras, *Annals Math.* **1953** 57, 591-603.
- [8] Yu. A. Neretin. An estimate of the number of parameters defining an n -dimensional algebra. *Math. USSR Izv.* **1988** 30(2), 283-294
- [9] Nijenhuis, A.; Richardson, R.W. Cohomology and deformations of algebraic structures. *Bull. Amer. Math. Soc.* **1964**, 70, 406-411.
- [10] A. Nijenhuis, R. W. Richardson. Cohomology and deformations in graded Lie algebras, *Bull. Amer. Math. Soc.* **72** (1966), 1-29.
- [11] Oviaño García, F. Sobre la rigidez de las álgebras de Lie reales resolubles reales de rango uno, Tesis Doctoral, Universidad Complutense de Madrid, 2024.

University Complutense of Madrid.
Email address: foviano@ucm.es

University Complutense de Madrid.
Email address: rutwig@ucm.es

DEALING WITH NON-PRINCIPAL LOCUS IN AUTOMATED REASONING IN GEOMETRY

ÁLVARO PEREIRA-ALBERT, TOMÁS RECIO, AND M. PILAR VÉLEZ

ABSTRACT. The integration of the computer algebra system Giac into GeoGebra opened the possibility of algebraically modeling a geometric construction made in GeoGebra and manipulating it with computer algebra algorithms, thus allowing the development of mathematically rigorous and high-performance Automatic Reasoning Tools (ART) to deal with geometric statements. Thus, the GeoGebra Discovery version of GeoGebra includes some advanced tools offering the user a rich variety of ART to experiment, discover and assert in geometric contexts. In this presentation, we deal with the performance of one of these tools, the LocusEquation command, for automatically discover how to modify a given figure so that an incorrect or unfinished statement becomes true, returning where to place some point in a construction so that a given property is satisfied. An easy and strange example, which GeoGebra Discovery has problems to compute because the locus ideal is not principal, yields some interesting problems (non-principal locus ideals, adding non-degeneracy conditions, interpretation of two simple, yet not trivial, locus) to deal with.

INTRODUCTION

Dynamic Geometry (DG) systems have become quite popular for teaching purposes. Although initially characterized by the ability to drag geometric constructions while keeping the relations (perpendicularity, parallelism, etc.) established by the user among the involved geometric objects, some of these environments evolved to integrate a computer algebra system, so they should be better described as “dynamic mathematics” software. This is the case of GeoGebra¹, integrating the computer algebra system Giac.

This has opened the possibility to translate algebraically the geometric relations between objects in a construction and, thus, to deal with computer algebra algorithms that allow the development of highly performing, mathematically rigorous (not just probabilistic or numerically approximate) Automatic Reasoning Tools (ART) on geometric statements([5, 9]). Thus, currently, GeoGebra (and, for some advanced tools, the fork version GeoGebra Discovery²) already offers the user a rich variety of ART for tasks related to experimenting, discovering, and asserting ([3, 6, 7, 8]):

- Automatically declaring the truth or failure of a given statement (**Prove** and **ProveDetails** commands),

The second and third authors have been partially supported by the grant “Mathematical Visualization: Foundations, Algorithms and Applications” PID2020-113192GB-I00 from the Spanish MICINN.

The talk at the meeting EACA 2024 has been given by the first author.

¹<http://www.geogebra.org>

²<https://github.com/kovzol/geogebra/releases>

- Automatically discovering how to modify a given figure so that a wrong statement becomes true (**LocusEquation** command, returning where to place some point on a construction so that a given property holds),
- Automatically discovering and returning a message with the properties holding among some selected pair of elements of the given figure (**Relation** command),
- Automatically discovering all statements (of a certain kind: lengths ratio, perpendicularity, etc.) holding true and involving a given element in a figure, selected/introduced by the user (**Discover**, **StepwiseDiscovery** command),
- Automatically discovering all statements of a certain kind involving “all” the elements of a given figure, see <https://autgeo.online/ag/automated-geometer.html?offline=1>,
- Displaying the different algebraic steps performed internally by the program to confirm or deny a given statement through the **ShowProof** command.

1. THE LOCUSEQUATION COMMAND

In this presentation, we are going to focus on the **LocusEquation** command ([1, 2, 4]). As stated before, given a geometrical construction, a property p for the construction and a point P , this command returns an equation that must be satisfied by the point P in order for the construction to satisfy the given property p . In other words, the **LocusEquation** command returns the equation for the geometric locus of points for which a given property is satisfied.

The command works as follows: First, it converts the geometrical construction into a set of polynomial equations, at least some of which should depend on the coordinates of the point P . It then considers the ideal generated by these polynomials, and performs an elimination of all variables except the coordinates of P , making use of the computer algebra system Giac (which is embedded into GeoGebra). We would expect this resulting elimination ideal to be principal, that is, we would obtain a single equation on the coordinates of P , which is the equation that P must satisfy in order to the property p to hold.

To visualize this, let us consider a simple example: Let the points A and B in the plane be $A = (0, 0)$ and $B = (1, 0)$, and we are going to search for the locus of points $P = (p_1, p_2)$ such that the line through P and B is perpendicular to the line through A and B . We would expect this command to return the equation for the line $x = 1$.

In this case, the equation of the line through A and B is $y = 0$, and the equation of the line through B and a point X with general coordinates $P = (p_1, p_2)$ is $p_2 x - (p_1 - 1)y = p_2$. Thus, the perpendicularity condition is given by the equation $-(p_1 - 1) = 0$, and in this case, we do not need to perform any elimination, since the ideal is already generated by a polynomial on the coordinates of the point P . Therefore, in order for those two lines to be perpendicular, we need the point P to satisfy the equation $p_1 = 1$, that is, it needs to lie on the line $x = 1$, which is the result that the **LocusEquation** command returns, as expected.

2. AN EASY EXAMPLE WITH A STRANGE OUTCOME

This presentation will be focused in another example, which is also geometrically simple to understand but uncovers some interesting problems when we try to solve it with GeoGebra Discovery: Given the triangle with vertices A , B and C , we look for the locus of the vertex C so that the Euler line of the triangle is perpendicular to the segment AB . In order to

simplify this computation, we can specialize the points A and B to be $A = (-1, 0)$ and $B = (1, 0)$. Geometrical intuition tells us that the answer should be for C to lie in the line given by $x = 0$. Since the Euler line is defined as the line that passes through three points related to the triangle (its barycentre, its circumcentre and its orthocentre), we can make this construction in GeoGebra in different ways, for instance:

- (1) We can first construct the orthocentre and the barycentre, and then define the Euler line to be the line passing through those two points.
- (2) Alternatively, we can construct the barycentre and the circumcentre, and let the Euler line be the line passing through those points.
- (3) Finally, we can construct the circumcentre and the orthocentre, and make the Euler line be the line defined by those points.

If we now try to compute the locus of the point C to satisfy the condition that the Euler line is perpendicular to the segment AB using the `LocusEquation` command, we would expect the result to be the same no matter the way we have defined the Euler line. However, this is not the case. In both the first and the second possible ways of making the construction above, the command outputs a polynomial of degree 5, and only in the third way described above we get the expected result. Figure 1 below shows the outcomes of these processes.

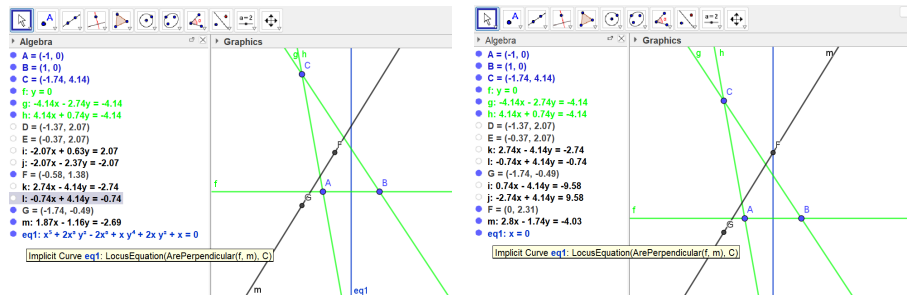


FIGURE 1. Output from the `LocusEquation` command when we construct the Euler line following the first way described above (left) and the third way (right). The triangle ABC is shown in green, the Euler line in black, and the output from the command in blue.

Now, if we copy on Maple (<https://www.maplesoft.com>) the set of equations that GeoGebra Discovery associates internally to the computation of the locus of $C = (v_9, v_{10})$ in the first construction, and we eliminate all variables except the coordinates of C , we get the ideal $\langle v_9 v_{10}, v_9^3 - v_9 \rangle$, that is, a non-principal ideal that factors as $\langle v_9 \rangle \cdot \langle v_{10}, v_9 - 1 \rangle \cdot \langle v_{10}, v_9 + 1 \rangle$. This means that the obtained locus includes points $A = (-1, 0)$, $B = (1, 0)$ plus the line $v_9 = 0$, i.e. $x = 0$, as expected. But GeoGebra Discovery internally represents point A as $y^2 + x^2 + 2x + 1 = 0$, point B as $y^2 + x^2 - 2x + 1 = 0$, thus the output of GeoGebra—as shown in the figure—is the degree five polynomial, product of the three factors:

$$x(y^2 + x^2 + 2x + 1)(y^2 + x^2 - 2x + 1) = x^5 + 2x^3y^2 - 2x^3 + xy^4 + 2xy^2 + x.$$

In this presentation we will analyse some of the strange behaviors appearing in this example, using, as above, symbolic computation software to obtain conclusions that allows us to improve the `LocusEquation` command in GeoGebra Discovery.

REFERENCES

- [1] M. Abánades, F. Botana, A. Montes, and T. Recio, *An algebraic taxonomy for locus computation in dynamic geometry*, Computer-Aided Design **56** (2014), 22–33, DOI 10.1016/j.cad.2014.06.008
- [2] J. Blazek, and P. Pech, *Searching for loci using GeoGebra*, International Journal for Technology in Mathematics Education **27** (2017), 143–147.
- [3] F. Botana, Z. Kovács, and T. Recio, *A mechanical geometer*, Mathematics in Computer Science **15** (2021) 631–641, DOI 10.1007/s11786-020-00497-7
- [4] F. Botana, and M. Abánades, *Automatic Deduction in (Dynamic) Geometry: Loci Computation*, Computational Geometry **47** (2014), no. 1, 75–89.
- [5] Z. Kovács, T. Recio, and M.P. Vélez, *Detecting truth, just on parts* Revista Matemática Complutense **32** (2019), 451–474, DOI 10.1007/s13163-018-0286-1
- [6] Z. Kovács, T. Recio, and M.P. Vélez, *Automated reasoning tools in GeoGebra Discovery*, ISSAC 2021 Software Presentations, ACM Communications in Computer Algebra **55** (2021), no. 2, Issue 216, 39–43, DOI 10.1145/3493492.3493495
- [7] Z. Kovács, T. Recio, and M.P. Vélez, *Automated reasoning tools with GeoGebra: What are they? What are they good for?*, In: P. R. Richard, M. P. Vélez, S. van Vaerenbergh (eds): *Mathematics Education in the Age of Artificial Intelligence: How Artificial Intelligence can serve mathematical human learning*. Series: Mathematics Education in the Digital Era, Springer, 2022, 23–44. DOI 10.1007/978-3-030-86909-0_2
- [8] Z. Kovács, T. Recio, and M.P. Vélez, *Showing proof, assessing difficulty with GeoGebra Discovery*. In: Quaresma, P. and Kovács, Z. (Eds.), Proceedings 14th International Conference on Automated Deduction in Geometry, Electronic Proceedings in Theoretical Computer Science 398, Open Publishing Association, 2023, 43–52, DOI 10.4204/EPTCS.398.8
- [9] T. Recio, and M.P. Vélez, *Automatic Discovery of Theorems in Elementary Geometry*. Journal of Automated Reasoning **23** (1999), 63–82, DOI 10.1023/A:1006135322108

Universidad Antonio de Nebrija

Email address: `apereiraa @ nebrija.es`

Universidad Antonio de Nebrija

Email address: `trecio @ nebrija.es`

Universidad Antonio de Nebrija

Email address: `pvelez @ nebrija.es`

EXPLORING THE DICRITICAL CONFIGURATIONS OF EXTENDED PLANAR FOLIATIONS

ELVIRA PÉREZ-CALLEJO

ABSTRACT. We study planar polynomial differential systems through considering foliations on the complex plane. We deal with the *algebraic integrability problem*, which asks for deciding whether a planar polynomial foliation has a rational first integral and to calculate it in the affirmative case. A classical procedure consists of the study of the resolution of the extended foliation to some compactification of the complex plane. Considering the projective plane and the Hirzebruch surfaces as compactifications, we explore the differences between the dicritical resolutions of the respective extended foliations.

1. PRELIMINARIES

1.1. Planar polynomial foliations. A foliation $\mathcal{F}$ on a smooth complex surface Z can be defined by a family of pairs $\{(U_i, \omega_i)\}_{i \in I}$, where $\{U_i\}_{i \in I}$ is an open covering of Z and, for all $i \in I$, ω_i is a non-zero regular differential 1-form such that, for any $i, j \in I$, $\omega_i = f_{ij}\omega_j$ on $U_i \cap U_j$ for some $f_{ij} \in \mathcal{O}_S(U_i \cup U_j)$ (see [2]).

Given a point $p \in U_i$, let $\omega_p = a_p(x, y)dx + b_p(x, y)dy$ be the local form of ω_i at p . The *algebraic multiplicity* of $\mathcal{F}$ at p is defined to be the integer $\nu_p(\mathcal{F}) = \min\{\text{ord}(a_p), \text{ord}(b_p)\}$. The *singularities* of $\mathcal{F}$ are the points p where $\nu_p(\mathcal{F}) \geq 1$. In this work any considered foliation has isolated singularities.

Given two coprime polynomials $P(x, y), Q(x, y) \in \mathbb{C}[x, y]$, the planar vector field $\mathcal{X} = P(x, y)\frac{\partial}{\partial x} + Q(x, y)\frac{\partial}{\partial y}$ can also be determined by the differential 1-form $\omega = Q(x, y)dx - P(x, y)dy$. It defines a planar polynomial foliation, which will be denoted by $\mathcal{F}^{\mathbb{C}^2}$.

1.2. Compactifications of the complex plane. The projective plane $\mathbb{P}^2$ can be regarded as the quotient $(\mathbb{C}^3 \setminus \{(0, 0, 0)\})/\sim$ where $(X, Y, Z) \sim (\lambda X, \lambda Y, \lambda Z)$ for all $\lambda \in \mathbb{C}^*$. The homogeneous coordinate ring of $\mathbb{P}^2$ is $\mathbb{C}[X, Y, Z]$ where all the variables are graded with degree 1. The projective plane can be covered by three affine open sets, U_X, U_Y and U_Z , defined as $U_A = \{(X : Y : Z) \in \mathbb{P}^2 \mid A \neq 0\}$, for $A = X, Y, Z$. We can identify each one of these affine open sets with $\mathbb{C}^2$. For example, in U_Z , $(X : Y : Z) = (X/Z : Y/Z : 1)$ so we can identify U_Z with $\mathbb{C}^2$ by means of the isomorphism $(X : Y : Z) \mapsto (x, y)$, where $x = X/Z$ and $y = Y/Z$.

Let $\delta \in \mathbb{Z}_{\geq 0}$. The δ th Hirzebruch surface is the projective space $\mathbb{F}_\delta := \mathbb{P}_{\mathbb{P}^1}(\mathcal{O}_{\mathbb{P}^1} \oplus \mathcal{O}_{\mathbb{P}^1}(\delta))$. $\mathbb{F}_\delta$ is a geometrically ruled surface over $\mathbb{P}^1$ that can be regarded as the quotient $(\mathbb{C}^2 \setminus \{(0, 0)\}) \times (\mathbb{C}^2 \setminus \{(0, 0)\})/\sim$ where $(X_0, X_1; Y_0, Y_1) \sim (\lambda X_0, \lambda X_1; \mu Y_0, \lambda^{-\delta}\mu Y_1)$ for all

The author has been partially supported by grant PID2022-138906NB-C22 funded by MICIU/AEI/10.13039/501100011033 and by ERDF/EU and by TED2021-130358B-I00 funded by MCIN/AEI/10.13039/501100011033 and by ERDF "A way of making Europe", as well as by grants GACU-JIMB/2023/03 and UJI-B2021-02 funded by Universitat Jaume I.

$(\lambda, \mu) \in \mathbb{C}^* \times \mathbb{C}^*$. The homogeneous coordinate ring of $\mathbb{F}_\delta$ is $\mathbb{C}[X_0, X_1, Y_0, Y_1]$ where the variables are graded on $\mathbb{Z} \times \mathbb{Z}_{\geq 0}$ as follows: $\deg(X_0) = \deg(X_1) = (1, 0)$, $\deg(Y_0) = (0, 1)$ and $\deg(Y_1) = (-\delta, 1)$. We say that a polynomial in $\mathbb{C}[X_0, X_1, Y_0, Y_1]$ is *homogeneous of degree* $(d_1, d_2) \in \mathbb{Z} \times \mathbb{Z}_{\geq 0}$ if it is a sum of terms $kX_0^{\alpha_0}X_1^{\alpha_1}Y_0^{\beta_0}Y_1^{\beta_1}$ with $\alpha_0 + \alpha_1 - \delta\beta_1 = d_1$, $\beta_0 + \beta_1 = d_2$ and $k \in \mathbb{C}^*$. $\mathbb{F}_\delta$ can be covered by four affine open sets, U_{ij} , $i, j \in \{0, 1\}$, defined as $U_{ij} = \{(X_0, X_1; Y_0, Y_1) \in \mathbb{F}_\delta | X_i \neq 0, Y_j \neq 0\}$. We can identify each one of these affine open sets with $\mathbb{C}^2$. For example, in U_{00} , $(X_0, X_1; Y_0, Y_1) = (1, X_1/X_0; 1, X_0^\delta Y_1/Y_0)$ so we can identify U_{00} with $\mathbb{C}^2$ by means of the isomorphism $(X_0, X_1; Y_0, Y_1) \mapsto (x, y)$, where $x = X_1/X_0$ and $y = X_0^\delta Y_1/Y_0$. Notice that $\mathbb{F}_0 \cong \mathbb{P}^1 \times \mathbb{P}^1$. One can read more about Hirzebruch surfaces in [1].

The Hirzebruch surfaces (for $\delta \neq 1$) together with the projective plane are (up to isomorphism) the relatively minimal rational surfaces. This means that any rational surface admits a birational morphism to one of them (see [1, Theorem V.10]).

1.3. Extended foliations. We will denote by $\mathcal{F}^{\mathbb{P}^2}$ (respectively, $\mathcal{F}^\delta$) a foliation on $\mathbb{P}^2$ (respectively, $\mathbb{F}_\delta$). These foliations have the advantage that they can be easily introduced by means of a global 1-form $\Omega_{\mathbb{P}^2} = AdX + BdY + CdZ$ (respectively, $\Omega_\delta = A_{\delta,0}dX_0 + A_{\delta,1}dX_1 + B_{\delta,0}dY_0 + B_{\delta,1}dY_1$) where $A, B, C \in \mathbb{C}[X, Y, Z]$ (respectively, $A_{\delta,0}, A_{\delta,1}, B_{\delta,0}, B_{\delta,1} \in \mathbb{C}[X_0, X_1, Y_0, Y_1]$) are homogeneous polynomials of certain degrees satisfying the Euler's condition $AX + BY + CZ = 0$ (respectively, $A_{\delta,0}X_0 + A_{\delta,1}X_1 - \delta B_{\delta,1}Y_1 = 0$ and $B_{\delta,0}Y_0 + B_{\delta,1}Y_1 = 0$). See [3] (respectively, [5]) for more information on these constructions.

Let S_0 be the projective plane $\mathbb{P}^2$ (respectively, the δ th Hirzebruch surface $\mathbb{F}_\delta$). Notice that $\{U_X, U_Y, U_Z\}$ (respectively, $\{U_{00}, U_{01}, U_{10}, U_{11}\}$) is an open covering of S_0 and consider the isomorphism $\mathbb{C}^2 \rightarrow U$, where $U = U_Z$ (respectively, $U = U_{00}$). Our procedure of *extending a planar polynomial foliation* $\mathcal{F}^{\mathbb{C}^2}$ defined by the 1-form ω to S_0 is based on taking (U, ω) as one of the pairs defining the foliation although it could have been done considering any other pair (V, ω) . The explicit algorithm to compute the global 1-form defining the extended foliation is described in [8, Subsection 1.5.1.] (respectively, [6] or [8, Subsection 2.3.1.]).

1.4. Dicritical reduction of singularities. Let $\mathcal{F}$ be a foliation on a smooth complex surface Z , p a singularity of $\mathcal{F}$ and assume that $\mathcal{F}$ is given at p , in local coordinates x and y , by the differential 1-form $\omega_p : a_p(x, y)dx + b_p(x, y)dy = \sum_{h=\nu_p(\mathcal{F})}^{\infty} \omega_{h,p}$, where $\omega_{h,p} = a_{h,p}dx + b_{h,p}dy$ is the h th homogeneous jet of ω_p . The point p is a *simple singularity* if $\nu_p(\mathcal{F}) = 1$ and the matrix

$$\begin{pmatrix} \frac{\partial b_{1,p}}{\partial x} & \frac{\partial b_{1,p}}{\partial y} \\ \frac{\partial a_{1,p}}{\partial x} & \frac{\partial a_{1,p}}{\partial y} \end{pmatrix}$$

has two eigenvalues λ_1, λ_2 such that $\lambda_1\lambda_2 \neq 0$ and $\frac{\lambda_1}{\lambda_2} \notin \mathbb{Q}_{\geq 0}$ or $\lambda_1\lambda_2 = 0$ and $\lambda_1^2 + \lambda_2^2 \neq 0$. Otherwise, p is an *ordinary singularity*. If p is an ordinary singularity that also satisfies the equality $xa_{\nu_p(\mathcal{F}),p} + yb_{\nu_p(\mathcal{F}),p} = 0$, we say that p is a *terminal dicritical singularity*. By [9], the ordinary singularities can be reduced by blowing up. The set of centers of the sequence $\pi_{\mathcal{F}}$ which reduces the terminal dicritical singularities of $\mathcal{F}$ is called *dicritical configuration* of $\mathcal{F}$ and it is denoted by $\mathcal{B}_{\mathcal{F}}$.

1.5. Rational first integrals of foliations. Let S be either $\mathbb{C}^2$, $\mathbb{P}^2$ or $\mathbb{F}_\delta$, for $\delta \in \mathbb{Z}_{\geq 0}$, and $\mathcal{F}$ a foliation on S defined by the 1-form Ω . A *rational first integral* of $\mathcal{F}$ is a non-constant

rational function $R = \frac{F}{G}$ such that $\Omega \wedge dR = 0$. We say that $\mathcal{F}$ is *algebraically integrable* if it admits a rational first integral.

If $r(x, y) = \frac{f}{g}$ is a rational first integral of a planar polynomial foliation $\mathcal{F}^{\mathbb{C}^2}$, then there exist two coprime homogeneous polynomials $F_{\mathbb{P}^2}, G_{\mathbb{P}^2} \in \mathbb{C}[X, Y, Z]$ (respectively, $F_{\mathbb{F}_\delta}, G_{\mathbb{F}_\delta} \in \mathbb{C}[X_0, X_1, Y_0, Y_1]$) of the same degree such that $R_{\mathbb{P}^2}(X, Y, Z) = \frac{F_{\mathbb{P}^2}}{G_{\mathbb{P}^2}}$ (respectively, $R_{\mathbb{F}_\delta}(X_0, X_1, Y_0, Y_1) = \frac{F_{\mathbb{F}_\delta}}{G_{\mathbb{F}_\delta}}$) is a rational first integral of $\mathcal{F}^{\mathbb{P}^2}$ (respectively, $\mathcal{F}^\delta$), the extended foliation of $\mathcal{F}^{\mathbb{C}^2}$ to $\mathbb{P}^2$ (respectively, $\mathbb{F}_\delta$). Moreover, $r(X/Z, Y/Z) = R_{\mathbb{P}^2}(X, Y, Z)$ and $r(X_1/X_0, X_0^\delta Y_1/Y_0) = R_{\mathbb{F}_\delta}(X_0, X_1, Y_0, Y_1)$. This justifies the search for rational first integrals of foliations on $\mathbb{P}^2$ or $\mathbb{F}_\delta$.

By [7], the existence of a rational first integral of a foliation $\mathcal{F}$ on S is equivalent to the fact that all reduced and irreducible $\mathcal{F}$ -invariant curves are precisely the irreducible components of an irreducible pencil $\mathcal{P}_\mathcal{F} = \langle F, G \rangle$ (we say that a pencil is irreducible when its general element is a reduced and irreducible curve). Moreover, F/G is a rational first integral of $\mathcal{F}$.

We study the dicritical reduction of singularities of a foliation because, by [4, Corollary 2] (proved for foliations on $\mathbb{P}^2$ and easily extensible to foliations on $\mathbb{F}_\delta$), $\mathcal{B}_\mathcal{F}$ coincides with the configuration of points which eliminates the base points of the pencil $\mathcal{P}_\mathcal{F}$, and therefore, it can provide information about a rational first integral of $\mathcal{F}$. We emphasise that the number of terminal dicritical divisors involved in the dicritical reduction affects the difficulty of the calculation of the first integral; the larger the number, the more difficult it becomes (see, for example, [8, Subsection 2.4.1]).

2. COMPARISON OF EXTENSIONS

We conclude by providing two examples showing that both the dicritical configuration and the number of terminal dicritical points depend on the extension, and usually change. Both examples show the proximity graph of the dicritical configuration of two different extensions, with the terminal dicritical points highlighted in red. For the construction of these examples, the software system Mathematica has been used.

Example 2.1. Let $\mathcal{F}^{\mathbb{C}^2}$ be an (algebraically integrable) polynomial foliation on $\mathbb{C}^2$ defined by the 1-form $\omega := (-6y - xy^3)dx + (-6x - x^3y)dy$ and consider the extended foliations $\mathcal{F}^{\mathbb{P}^2}$ and $\mathcal{F}^0$, to $\mathbb{P}^2$ and $\mathbb{F}_0$, respectively.



FIGURE 1. Proximity graph of $\mathcal{B}_{\mathcal{F}^{\mathbb{P}^2}}$ (on the left) and $\mathcal{B}_{\mathcal{F}^0}$ (on the right)

The left-hand side of Figure 1 shows the proximity graph of the dicritical configuration of the foliation $\mathcal{F}^{\mathbb{P}^2}$ while the right-hand side shows the proximity graph of the dicritical configuration of $\mathcal{F}^0$. We see that extending to $\mathbb{F}_0$ instead of $\mathbb{P}^2$, the number of terminal dicritical divisors (and hence, the difficulty of the computation of a rational first integral) decreases.

Example 2.2. Let $\mathcal{F}^{\mathbb{C}^2}$ be an (algebraically integrable) polynomial foliation on $\mathbb{C}^2$ defined by the 1-form $\omega := (-1-4x^3+3y+4x^3y-3y^2+y^3)dx + (-2-2x-4x^4+4y+4xy-2y^2-2xy^2)dy$ and consider the extended foliations $\mathcal{F}^{\mathbb{P}^2}$ and $\mathcal{F}^2$ to $\mathbb{P}^2$ and $\mathbb{F}_2$, respectively.

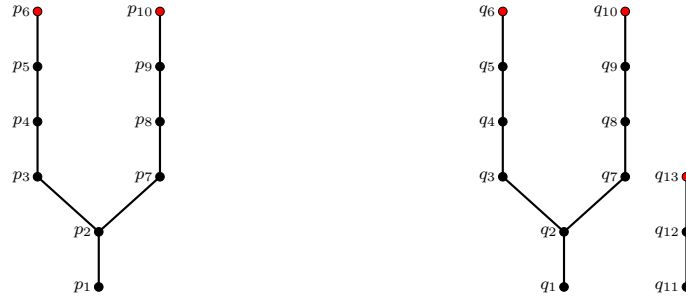


FIGURE 2. Proximity graphs of $\mathcal{B}_{\mathcal{F}^{\mathbb{P}^2}}$ (on the left) and $\mathcal{B}_{\mathcal{F}^2}$ (on the right)

In this case, extending to $\mathbb{F}_2$ instead of $\mathbb{P}^2$ increases the number of terminal dicritical divisors (and hence, the difficulty of the computation of a rational first integral).

REFERENCES

- [1] A. Beauville. *Complex Algebraic Surfaces*, London Math. Soc. Student Texts. Cambridge University Press, Cambridge, **34(2)**, 1996.
- [2] M. Brunella. *Birational Geometry of Foliations*. IMPA Monogr. Springer, 2015.
- [3] A. Campillo and J. Olivares. Polarity with respect of a foliation and Cayley-Bacharach Theorems. *J. Reine Angew. Math.*, 534:95–118, 2001.
- [4] A. Ferragut, C. Galindo, and F. Monserrat. A class of polynomial planar vector fields with polynomial first integral. *J. Math. Anal. Appl.*, 430(1):354–380, 2015.
- [5] C. Galindo, F. Monserrat, and J. Olivares. Foliations with isolated singularities on Hirzebruch surfaces. *Forum Math.*, 33(6):1471–1483, 2021.
- [6] C. Galindo, F. Monserrat and E. Pérez-Callejo. Algebraic integrability of planar polynomial vector fields by extension to Hirzebruch surfaces, *Qual. Theory Dyn. Syst.* **21(126)**, 2022.
- [7] J.P. Jouanolou. *Equations de Pfaff Algébriques*, volume 708 of Lecture Notes in Math. Springer, Verlag, 1979.
- [8] E. Pérez-Callejo. Algebraic integrability of foliations by extension to Hirzebruch surfaces. Applications to bounded negativity, *PhD Thesis, Departament de Matemàtiques, Universitat Jaume I*. 2023.
- [9] A. Seidenberg. Reduction of singularities of the differentiable equation $Ady = Bdx$. *Amer. J. Math.*, 90:248–269, 1968.

University Jaume I

Email address: callejo@uji.es

GENERALIZED ASYMPTOTES OF PARAMETRIC CURVES

SONIA PÉREZ-DÍAZ

ABSTRACT. We obtain a simple formula based on the computation of some derivatives for determining the asymptotes of curves that are defined by a rational parametrization. For this purpose, we use some previous results and notions presented in [1], [2], [3] and [4]. We develop this method for the plane case but it can be adapted for rational curves in the n -dimensional space. In addition, the formulas presented can be similarly obtained for curves defined by a parametrization not necessarily rational.

INTRODUCTION

In this paper we present an algorithmic solution that allows to determine the behavior at infinity of a plane parametric curve, $\mathcal{C}$, by calculating the generalized asymptotes of its branches at points with sufficiently large coordinates. This concept generalizes the classical concept of asymptote and its methods of calculation.

Intuitively, given a curve $\mathcal{C}$, $\tilde{\mathcal{C}}$ is said to be a *g-asymptote* of $\mathcal{C}$, if $\tilde{\mathcal{C}}$ is a curve of the smallest possible degree that approximates $\mathcal{C}$ at infinity (see [1, 2]). The method presented in Section 3 is based on the preliminary studies in Section 1, as well as on the concepts of *perfect curve* and *g-asymptote* defined in Section 2.

It should be noted that the novelties with respect to previous works are based on an improvement and implementation of the results presented here, illustrating them by means of an algorithm based on the calculation of some derivatives in one variable. More precisely, the novelty lies in the explicit formulas displayed in Theorem 3.1, which allow the computation of the g-asymptotes of a curve defined by a parametrization by merely determining some simple derivatives of functions constructed from the input parametrization.

1. NOTATION AND PRELIMINARIES

In the following, we introduce some basic notions as the concept of *infinity branch*, *convergent branches* and *approaching curves*, obtained from some previous results (see [1, 2, 4]).

We consider an irreducible algebraic affine plane curve $\mathcal{C}$ over $\mathbb{C}$ defined by the irreducible polynomial $f(x, y) \in \mathbb{R}[x, y]$. Let $\mathcal{C}^*$ be its corresponding projective curve, defined by the homogeneous polynomial $F(x, y, z) = f_d(x, y) + zf_{d-1}(x, y) + z^2f_{d-2}(x, y) + \dots + z^df_0 \in \mathbb{R}[x, y, z]$, where $d := \deg(\mathcal{C})$ and f_i are homogeneous polynomials of degree i , $i \in \{0, \dots, d\}$. We assume that $(0 : 1 : 0)$ is not an infinity point of $\mathcal{C}^*$ (otherwise, we may consider a linear change of coordinates). In order to get the *infinity branches* of $\mathcal{C}$, we consider the curve defined by the polynomial $g(y, z) = F(1 : y : z)$ and we compute the Puiseux series, φ_i , $i = 1 \dots \deg_y(g)$ of $g(y, z) = 0$ around $z = 0$ ([2]). In the following, we denote by $\varphi(t) = m + a_1t^{N_1/N} + a_2t^{N_2/N} + a_3t^{N_3/N} + \dots$, $a_i \neq 0, \forall i \in \mathbb{N}$, with $N_i \in \mathbb{N}$, $i = 1, \dots$,

Author is partially supported by Ministerio de Ciencia, Innovación y Universidades -Agencia Estatal de Investigación/PID2020-113192GB-I00 (Mathematical Visualization: Foundations, Algorithms and Applications). Author belongs to the Research Group ASYNACS (Ref. CCEE2011/R34).

and $0 < N_1 < N_2 < \dots$ one of these series. Then, $g(\varphi(t), t) = 0$ in some neighborhood of $z = 0$ where $\varphi(z)$ converges.

Definition 1.1. An *infinity branch* of an affine plane curve $\mathcal{C}$ associated to the infinity point $P = (1 : m : 0)$, $m \in \mathbb{C}$, is a set $B = \{(z, r(z)) \in \mathbb{C}^2 : z \in \mathbb{C}, |z| > M\}$, where $r(z) = z\varphi(z^{-1}) = mz + a_1z^{1-N_1/N} + a_2z^{1-N_2/N} + a_3z^{1-N_3/N} + \dots$ and $M \in \mathbb{N}$.

Definition 1.2. Given two *branches*, $B = \{(z, r(z)) \in \mathbb{C}^2 : z \in \mathbb{C}, |z| > M\}$ and $\bar{B} = \{(z, \bar{r}(z)) \in \mathbb{C}^2 : z \in \mathbb{C}, |z| > \bar{M}\}$, we say that they *converge* if $\lim_{z \rightarrow \infty} (\bar{r}(z) - r(z)) = 0$.

Definition 1.3. Let $\mathcal{C}$ be an algebraic plane curve with an infinity branch B . We say that a curve $\bar{\mathcal{C}}$ *approaches* $\mathcal{C}$ at its infinity branch B if $\lim_{z \rightarrow \infty} d((z, r(z)), \bar{\mathcal{C}}) = 0$

[2] shows that if $\mathcal{C}$ is a plane curve with an infinite branch B then, a plane curve $\bar{\mathcal{C}}$ approximates $\mathcal{C}$ at B iff $\bar{\mathcal{C}}$ has an infinite branch $\bar{B}$ such that B and $\bar{B}$ are convergent.

2. GENERALIZED ASYMPTOTES AND PERFECT CURVES

From the concepts introduced in Section 1, we get the following definitions (see [1]).

Definition 2.1. An algebraic curve of degree d is a *perfect curve* if it cannot be approached by any curve of degree less than d .

A curve that is not perfect can be approached by other curves of smaller degree. If these curves are perfect, we call them *g-asymptotes*.

Definition 2.2. Let $\mathcal{C}$ be a curve with an infinity branch B . A *g-asymptote* (generalized asymptote) of $\mathcal{C}$ at B is a perfect curve that approaches $\mathcal{C}$ at B .

Let $\mathcal{C}$ be with a branch $B = \{(z, r(z)) \in \mathbb{C}^2 : z \in \mathbb{C}, |z| > M\}$, where $r(z) = mz + a_1z^{1-N_1/N} + \dots + a_kz^{1-N_k/N} + a_{k+1}z^{1-N_{k+1}/N} + \dots$, with $a_1, a_2, \dots \in \mathbb{C} \setminus \{0\}$, $m \in \mathbb{C}$, $N, N_1, N_2, \dots \in \mathbb{N}$, and $0 < N_1 < N_2 < \dots$. Assume that $N_k \leq N < N_{k+1}$ that is, the terms $a_jz^{1-N_j/N}$ with $j \geq k+1$ have negative exponent. In the following, we write $r(z) = mz + a_1z^{1-n_1/n} + \dots + a_kz^{1-n_k/n} + a_{k+1}z^{1-N_{k+1}/N} + \dots$ with $\gcd(N, N_1, \dots, N_k) = b$, $N_j = n_jb$, $N = nb$, $j = 1, \dots, k$. That is, we simplify the exponents such that $\gcd(n, n_1, \dots, n_k) = 1$. Note that $0 < n_1 < n_2 < \dots$, $n_k \leq n$, and $N < n_{k+1}$, i.e. the terms $a_jz^{1-N_j/N}$ with $j \geq k+1$ have negative exponent. Let $\tilde{r}(z) = mz + a_1z^{1-n_1/n} + \dots + a_kz^{1-n_k/n}$ be the terms with non-negative exponent of $r(z)$. We consider $z = t^n$, to get the proper parametrization of the curve $\tilde{\mathcal{C}}$, $\tilde{\mathcal{P}}(t) = (t^n, mt^n + a_1t^{n-n_1} + \dots + a_kt^{n-n_k}) \in \mathbb{C}[t]^2$, where $n, n_1, \dots, n_k \in \mathbb{N}$, $\gcd(n, n_1, \dots, n_k) = 1$, and $0 < n_1 < \dots < n_k$, is a g-asymptote of $\mathcal{C}$ ([1]).

Now, we present a method to compute g-asymptotes of a plane curve from their parametric (rational) representation. This method is included in [3] and it involves the computation of Puiseux series. In Section 3, we develop a new method that allows to easily compute the g-asymptotes by only determining some derivatives of rational functions constructed from the given parametrization ([4]). Let $\mathcal{C}$ be a plane curve defined by the rational parametrization $\mathcal{P}(s) = (p_1(s), p_2(s))$, $p_i(s) = p_{i1}(s)/p_{i2}(s)$, $\gcd(p_{i1}, p_{i2}) = 1$, $i = 1, 2$. A parametrization of $\mathcal{C}^*$ is given by $\mathcal{P}^*(s) = (1 : p_2(s)/p_1(s) : 1/p_1(s))$.

In order to compute the g-asymptotes of $\mathcal{C}$, first we need to determine the infinity branches $B = \{(z, r(z)) \in \mathbb{C}^2 : z \in \mathbb{C}, |z| > M\}$, where $r(z) = z\varphi(z^{-1})$. From Definition 1.1, we

have that $f(z, r(z)) = F(1 : \varphi(t) : t) = 0$ around $t = 0$, where $t = z^{-1}$. Now, we have the parametrization $\mathcal{P}^*$ and then $F(1 : p_2(s)/p_1(s) : 1/p_1(s)) = 0$. Hence, in order to compute the infinity branches of $\mathcal{C}$, and in particular φ , one needs to rewrite $\mathcal{P}^*(s)$ in the form $(1 : \varphi(t) : t)$ around $t = 0$. For this purpose, we look for a value of the parameter s , say $\ell(t) \in \mathbb{C}\langle\langle t \rangle\rangle$ ($\mathbb{C}\langle\langle t \rangle\rangle$ denotes the field of formal Puiseux series), such that $\mathcal{P}^*(\ell(t)) = (1 : \varphi(t) : t)$ around $t = 0$. Hence, we have to consider the equation $1/p_1(s) = t$ (equivalently, $p_{12}(s) - tp_{11}(s) = 0$), and then we solve it in the variable s around $t = 0$. From Puiseux's Theorem, there exist $\ell_i(t) \in \mathbb{C}\langle\langle t \rangle\rangle$ such that, $p_{12}(\ell_i(t)) - tp_{11}(\ell_i(t)) = 0$, $i \in \{1, \dots, k\}$, in a neighborhood of $t = 0$. For each $i \in \{1, \dots, k\}$, there exists $M_i \in \mathbb{R}^+$ such that the points $(1 : \varphi_i(t) : t)$ (equivalently, $(t^{-1} : t^{-1}\varphi_i(t) : 1)$), where $\varphi_i(t) = p_2(\ell_i(t))/p_1(\ell_i(t))$, are in $\mathcal{C}^*$ for $|t| < M_i$. We set $z = t^{-1}$ to get $(z, r_i(z))$, where $r_i(z) = z\varphi_i(z^{-1})$, are in $\mathcal{C}$ for $|z| > M_i^{-1}$. Hence, the infinity branches are $B_i = \{(z, r_i(z)) \in \mathbb{C}^3 : z \in \mathbb{C}, |z| > M_i^{-1}\}$, $i \in \{1, \dots, k\}$. Note that $p_1(\ell_i(t))t = 1$, for $i \in \{1, \dots, k\}$ and then $\varphi_i(t) = p_2(\ell_i(t))/p_1(\ell_i(t)) = p_2(\ell_i(t))t$, $r_i(z) = z\varphi_i(z^{-1}) = p_2(\ell_i(z^{-1}))$. Once we have the infinity branches, we can compute a g-asymptote by simply removing the terms with negative exponent from r_i .

3. COMPUTATION OF G-ASYMPTOTES OF PARAMETRIC CURVES USING DERIVATIVES

In this section, we present a method that allows us to easily compute all the g-asymptotes of a curve defined by a parametrization by only determining some simple derivatives of functions constructed from the input parametrization. Although the formulas obtained in Theorem 3.1 are new, the main idea for proving this theorem using some previous and well-established results can be found in [4].

Theorem 3.1. *Let $\mathcal{C}$ be a curve defined by a parametrization $\mathcal{P}(s) = (q_1(s), q_2(s)) \in \mathbb{R}(s)^2$, where $q_i(s) = p_i(s)/p(s)$, and $\gcd(p_1, p_2, p) = 1$, $i = 1, 2$. Let $\tau \in \mathbb{C}$ be such that we write $p(t) = (t - \tau)^n \bar{p}(t)$ where $\bar{p}(\tau)p_1(\tau) \neq 0$, $i = 1, 2$, and $n \geq 1$. Let B be the corresponding infinity branch. A g-asymptote of B is defined by $\tilde{\mathcal{P}}(t) = (t^n, a_n t^n + a_{n-1} t^{n-1} + \dots + a_0)$, where $a_n = \frac{p_2(\tau)}{p_1(\tau)}$, $a_i = \frac{1}{(n-i)!} \cdot \frac{\partial^{n-1-i}}{\partial t^{n-1-i}} \left(\frac{\partial}{\partial t} \left(\frac{p_2(t)}{p_1(t)} \right) \cdot \left(\frac{p_1(t)}{\bar{p}(t)} \right)^{(n-i)/n} \right) (\tau)$, $0 \leq i \leq n-1$.*

Example 3.1. *Let $\mathcal{C}$ be the plane curve defined by the parametrization*

$$\mathcal{P}(s) = \left(\frac{s^4 - s^3 + 5s^2 + 2s + 1}{s^4(s-1)(s-2)}, \frac{1/27(-108 - 216s + 27s^4 - 367s^3 - 2440s^2)}{s^4(s-1)(s-2)} \right) \in \mathbb{R}(s)^2.$$

We compute the g-asymptotes of $\mathcal{C}$ using Theorem 3.1. For this purpose, we first observe that $p_3(s)$ has the roots $\tau_1 = 1$, $\tau_2 = 2$, $\tau_3 = 0$, with multiplicities $n_1 = n_2 = 1$, and $n_3 = 4$. They provide the infinity points $(1 : -388/27 : 0)$ (for τ_1, τ_2) and $(1 : -4 : 0)$ (for τ_3).

For $\tau_1 = 1$, let $r(s) := 1/27(-108 - 216s + 27s^4 - 367s^3 - 2440s^2)/(s^4(s-2))$, $\ell(s) := 1/27(-108 - 216s + 27s^4 - 367s^3 - 2440s^2)/(s^4 - s^3 + 5s^2 + 2s + 1)$, $a_1 = \ell(1) = -388/27$, $a_0 = \frac{\partial \ell}{\partial t}(1)r(1) = -405460/729$. Then, we obtain the g-asymptote $\tilde{\mathcal{C}}_1$, defined by the proper parametrization $\tilde{\mathcal{P}}_1(t) = (t, -388/27t + 1045/27)$.

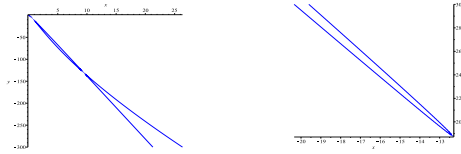
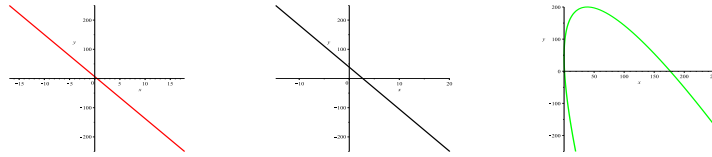
For $\tau_2 = 2$, we get $r(s) := 1/27(-108 - 216s + 27s^4 - 367s^3 - 2440s^2)/(s^4(s-1))$, and $a_1 = \ell(2) = -388/27$, $a_0 = \frac{\partial \ell}{\partial t}(2)r(2) = -67415/729$. Then, we obtain the g-asymptote $\tilde{\mathcal{C}}_2$, defined by the proper parametrization $\tilde{\mathcal{P}}_2(t) = (t, -388/27t + 695/108)$.

For $\tau_3 = 0$, $r(s) := (1/27(-108 - 216s + 27s^4 - 367s^3 - 2440s^2))^{1/4}/((s-1)^{1/4}(s-2)^{1/4})$,

$$a_4 = \ell(0) = -4, \quad a_3 = \frac{\partial \ell}{\partial t}(0)r(0) = 0, \quad a_2 = \frac{1}{2!} \cdot \frac{\partial}{\partial t} \left(\frac{\partial \ell(t)}{\partial t} \cdot r(t)^2 \right) (0) = 950/27\sqrt{2},$$

$$a_1 = \frac{1}{3!} \cdot \frac{\partial^2}{\partial t^2} \left(\frac{\partial \ell(t)}{\partial t} \cdot r(t)^3 \right) (0) = 0, \quad a_0 = \frac{1}{4!} \cdot \frac{\partial^3}{\partial t^3} \left(\frac{\partial \ell(t)}{\partial t} \cdot r(t)^4 \right) (0) = 6535/144.$$

The g -asymptote $\tilde{\mathcal{C}}_3$ is defined by $(t^4, -4t^4 + 950/27\sqrt{2}t^2 + 3080665/2916)$ that can be properly reparametrize as $\tilde{\mathcal{P}}_3(t) = (t^2, -4t^2 + 950/27\sqrt{2}t + 6535/144)$.

FIGURE 1. Curve $\mathcal{C}$.FIGURE 2. Asymptotes of the curve $\mathcal{C}$.FIGURE 3. Curve $\mathcal{C}$ and g -asymptotes.

REFERENCES

1. A. Blasco, S. Pérez-Díaz, *Asymptotes and Perfect Curves*. C. Aided G. Design, (2) **31**, 81—96. 2014.
2. A. Blasco, S. Pérez-Díaz, *Asymptotic Behavior of an Implicit Algebraic Plane Curve*. C. Aided G. Design, (7-8) **31**, 345—357. 2014.
3. A. Blasco, S. Pérez-Díaz, *Asymptotes of Space Curves*. J. Computational and Applied Mathematics, 278, 231—247. 2015.
4. S. Pérez-Díaz, M. Fernández de Sevilla, E. Campo, *A simple formula for the computation of branches and asymptotes of curves and some applications*. C. Aided G. Design, 102084. 2022.

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

A REAL MECHANICAL GEOMETER (EXTENDED ABSTRACT)

TOMÁS RECIO AND M. PILAR VÉLEZ

ABSTRACT. In our talk we introduce, first the current performance of the programs GeoGebra and GeoGebra Discovery regarding some automatic reasoning tools features, that use computational algebraic geometry methods, mostly in the complex setting. Then we focus on the pending theoretical and algorithmic issues to extend (in the same technological and educational framework) such methods to deal with statements in the real algebraic geometry context.

1. THE AUTOMATED GEOMETER IN GEOGEBRA AND GEOGEBRA DISCOVERY: CURRENT PERFORMANCE

Along the past decade we have worked towards the development of a kind of *Automated Geometer* ([1, 8, 10]), initially implemented on the popular program GeoGebra (www.geogebra.org).

Thus, the general version of GeoGebra –with more that 100 million users all over the world– includes already some *automated reasoning* tools (using and implementing partially some of the algorithms mentioned in the previous references). For example, GeoGebra is capable of

- finding an equality relation between two given geometric objects in a construction (i.e. of formulating a thesis holding under the set of hypotheses describing the geometric construction),
- of checking the truth/failure of a conjectured (by the user) relation,
- or finding missing hypotheses for a given relation to hold true.

The performance of these GeoGebra automated reasoning tools is quite impressive (as highlighted in the initially mentioned references). But, we want to focus here in the fact that GeoGebra commands, for proving or finding geometric properties, have some limitations that have been addressed in the fork version of GeoGebra named GeoGebra Discovery. GeoGebra Discovery (see <https://kovzol.github.io/geogebra-discovery/> for further details) extends GeoGebra tools by including new features (see [4, 5, 7, 9] for details and examples):

- finding the relation between two given geometric objects in a construction, including, in the case of lengths, the *discovery of relations that are not of equality*: obtaining algebraic number ratios, or inequality relations, through comparison,

The authors have been partially supported by the grant “Mathematical Visualization: Foundations, Algorithms and Applications” PID2020-113192GB-I00 from the Spanish MICINN.

The talk at the meeting EACA 2024 has been given by both authors.

- of checking the truth/failure of a conjectured (by the user) relation *involving inequalities* (e.g. $a^6 + b^6 + c^6 \geq 5148r^6$, related to an AMS-Monthly Problem, involving the sides of a triangle and the radius r of the incircle, see [13])
- discovering automatically all possible relations of a certain kind (co-circularity, parallelism, perpendicularity, etc) among the elements of a construction involving a chosen element, or all of them,
- the possibility, through the *ShowProof* command [11], of displaying in the GeoGebra Discovery CAS window the different algebraic steps internally performed by the program to confirm or deny a given statement,
- as well as a *measure of the complexity* of the proved statement, defined (see [11] for details) as the maximum degree of the polynomials f_i , such that $t = f_1 h_1 + \dots + f_r h_r$, or such that $1 = f_1 h_1 + \dots + f_r h_r + f_{r+1} * (zt - 1)$, where t is the thesis and $h_1, \dots, h_r$ are the hypotheses.

These improvements required, in particular, the porting, on a web platform and to GeoGebra Discovery, of the software program Tarski (<https://www.usna.edu/Users/cs/wcbrown/tarski/index.html>, <https://matek.hu/zoltan/tarski/webtarski.html>), for performing the required real quantifier elimination algorithms, see [7] for details.

2. A REAL AUTOMATED GEOMETER

The previous, summary, description of the current automated reasoning features of GeoGebra and GeoGebra discovery, did not include any reference to some subtle, but core, issues ruling the implemented protocols and algorithms. Within the space limitations of this extended abstract, let us roughly declare (referring to [12, 8, 4] for details and references) that dealing with a statement such as $\{h_1 = 0, \dots, h_r = 0\} \Rightarrow t = 0$

- *cannot* be approached simply by considering that it is true iff t belongs to the ideal of the zeroes of $(h_1, \dots, h_r)$ (using the corresponding Nullstellensatz, when working over the complex or over the real numbers). Indeed, most statements require to handle (to define, to get rid off) the *degenerate* instances that rise, unexpectedly, in the algebraic formulation of practically any statement. This involves
- selecting (perhaps by the user or automatically, following the steps of the geometric construction) a collection of variables equal to the (topological, Hilbert) dimension of the algebraic variety defined by the hypotheses,
- considering as non-degenerate components those where such variables remain independent
- labeling as *algebraically/geometrically/generally/partially* true those statements where the thesis *belongs to the ideal of hypotheses/vanishes over the whole hypotheses variety/or at least over all the non-degenerate components/or at most over some, but not all such components*. Let us remark that, in practice, it is quite common, and illustrative, to learn which of these cases holds for a given statement.
- detecting each of these cases without having to compute the ideal of the hypotheses variety or its components, but simply proceeding by checking if the output of some elimination algorithm is or not zero,
- obtaining, in the generally true case, some degeneracy conditions that should be avoided for the statement to be geometrically true,

- computing the *complexity* of a geometrically true statement by expressing 1 as an element of the ideal generated by the hypotheses and the negation $zt - 1$ of the thesis, after computing its normal form (0) with respect to a Gröbner basis of this ideal, and then expressing each element of this basis as a combination of the given generators.

It is well known (see [4]) that there are relevant coincidences (and differences) regarding the concept of truth for elementary geometry statements, if considered in the complex or real settings (for the zeroes of the involved hypotheses and thesis algebraic varieties). Many statements that hold true (in some of the senses defined above) over the reals hold as well over the complexes, so it is advisable to proceed, first, to verify its truth over the latter field, as it is easier, computationally speaking. Yet, our on-going research work aims to develop a similar theoretical framework to the one described above,

- specifically adapted to the case of real zeroes, including the case of statement dealing with inequalities (in the hypotheses, in the thesis), and handling an equivalent notion to *non-degenerate component* for semi-algebraic hypotheses sets.
- without having to compute the real radical, or the real irreducible components, for detecting the *generally true, etc.* case.
- replacing the *elimination* protocol of the complex case by a certain projection (i.e. a basic elimination of quantifiers), where we might be interested just in learning if such projection is contained, or not, on a proper, real hypersurface.
- keeping the (complex) notion of complexity, but this time considering, for its computation, the polynomials appearing in the real Nullstellensatz or Positivstellensatz, expressing that a given element belongs to the real radical of an ideal, or that it is zero, positive, strictly positive, etc. over a semialgebraic set.

We consider that this list of on-going tasks for developing a truly performing *real automated geometer* involve several, elementary, real algebraic geometry (RAG) issues that we are currently unable to address from a *practical* algorithmic perspective. Presenting the basic ideas of our project, to get some feedback from the EACA scientific community, is the final goal of our communication.

REFERENCES

- [1] M. Abánades, F. Botana, Z. Kovács, T. Recio, and C. Sólyom-Gecse, *Development of automatic reasoning tools in GeoGebra*, ACM Communications in Computer Algebra **50** (2016), no. 3, 85–88, DOI 10.1145/3015306.3015309
- [2] F. Botana, Z. Kovács, and T. Recio, *A mechanical geometer*, Mathematics in Computer Science **15** (2021) 631–641, DOI 10.1007/s11786-020-00497-7
- [3] P. Boutry, G. Braun, and J. Narboux, *Formalization of the arithmetization of Euclidean plane geometry and applications*, Journal of Symbolic Computation **90** (2019), 149–168, DOI 10.1016/j.jsc.2018.04.007
- [4] C. Brown, Z. Kovács, T. Recio, R. Vajda, and M.P. Vélez, *Is Computer Algebra Ready for Conjecturing and Proving Geometric Inequalities in the Classroom?* Mathematics in Computer Science **16** (2022), no. 31, DOI 10.1007/s11786-022-00532-9
- [5] C. Brown, Z. Kovács, T. Recio, R. Vajda, R., and M.P. Vélez, *GeoGebra Discovery*, In: C. Dubois, M. Kerber (eds), Intelligent Computer Mathematics, Proceedings of the 16th International Conference CICM, Lecture Notes in Computer Science, Springer 2023, DOI 10.1007/978-3-031-42753-4
- [6] A. Dolzmann, T. Sturm, and V. Weispfenning, *A new approach for automatic theorem proving in real geometry*. Journal of Automated Reasoning **21** (1998), no.3, 357–380, DOI 10.1023/A:1006031329384

- [7] Z. Kovács, C. Brown, T. Recio, and R. Vajda, *Computing with Tarski formulas and semi-algebraic sets in a web browser*, Journal of Symbolic Computation **120** (2024), 102235, DOI 10.1016/j.jsc.2023.102235
- [8] Z. Kovács, T. Recio, and M.P. Vélez, *Detecting truth, just on parts* Revista Matemática Complutense **32** (2019), 451–474, DOI 10.1007/s13163-018-0286-1
- [9] Z. Kovács, T. Recio, and M.P. Vélez, *Automated reasoning tools in GeoGebra Discovery*, ISSAC 2021 Software Presentations, ACM Communications in Computer Algebra **55** (2021), no. 2, Issue 216, 39–43, DOI 10.1145/3493492.3493495
- [10] Z. Kovács, T. Recio, and M.P. Vélez, *Automated reasoning tools with GeoGebra: What are they? What are they good for?*, In: P. R. Richard, M. P. Vélez, S. van Vaerenbergh (eds): *Mathematics Education in the Age of Artificial Intelligence: How Artificial Intelligence can serve mathematical human learning*. Series: Mathematics Education in the Digital Era, Springer, 2022, 23–44. DOI 10.1007/978-3-030-86909-0_2
- [11] Z. Kovács, T. Recio, and M.P. Vélez, *Showing proof, assessing difficulty with GeoGebra Discovery*. In: Quaresma, P. and Kovács, Z. (Eds.), Proceedings 14th International Conference on Automated Deduction in Geometry, Electronic Proceedings in Theoretical Computer Science 398, Open Publishing Association, 2023, 43–52, DOI 10.4204/EPTCS.398.8
- [12] T. Recio, and M.P. Vélez, *Automatic Discovery of Theorems in Elementary Geometry*. Journal of Automated Reasoning **23** (1999), 63–82, DOI 10.1023/A:1006135322108
- [13] D. Sitaru, *Problem 11984*. American Mathematical Monthly **124** (2017), no. 5, 466, <http://www.jstor.org/stable/10.4169/amer.math.monthly.124.5.465>

Universidad Antonio de Nebrija, Madrid, Spain.

Email address: trecio@nebrija.es

Universidad Antonio de Nebrija, Madrid, Spain.

Email address: pvelez@nebrija.es

USING EXPLAINABLE AI TO EXTRACT INSIGHTS ON ALGEBRAIC PROCEDURES: A CASE STUDY ON VARIABLE ORDERING FOR CAD

TERESO DEL RÍO ALMAJANO

ABSTRACT. Machine learning models have been successfully used to optimise computational algebra algorithms; wouldn't it be great if we could extract mathematical insights from them? We will explore how explainable AI (XAI) techniques can determine which features have the greatest impact on the decisions made by trained machine learning models. Then, we will use these features to develop new heuristics of a size and complexity similar to those human-designed heuristics currently commonly used that can be easily coded, avoiding computer algebra implementations from calling, and therefore creating dependencies, on AI tools.

1. OUR CASE STUDY: CHOOSING VARIABLE ORDERING FOR CAD

We present the algorithm of Cylindrical Algebraic Decomposition (CAD), the impact that the variable ordering can have in its complexity and how researchers have trained machine learning models to choose which variable ordering to use.

1.1. Cylindrical Algebraic Decomposition and the importance of Variable Ordering. CAD is an algorithm with multiple applications whose potential is strongly limited by its high computational complexity. This algorithm has a doubly exponential complexity in the number of variables, that is, the cost of building a CAD increases as more variables are added in a similar way to the number of wheat grains in Figure 1.

Nevertheless, [1] proved that the complexity of this algorithm was strongly dependant on the variable ordering chosen (in which order we study the variables). In fact, they discovered some polynomials for which a bad variable resulted in a doubly exponential computational complexity, while a good variable ordering had a constant complexity, that is, remained the same regardless of the number of variables. Therefore, choosing developing strategies to choose the right variable ordering might have an impact on the average complexity of CAD and therefore on its potential use on applications.

1.2. Machine Learning Models for Choosing the Variable Ordering. To train machine learning models we used a slight modification (balancing the training dataset, see [2]) of the machine learning methodology presented by Florescu and England [4].

This methodology generates multiple features to describe each set of polynomials to the machine learning models [3]. One of the features they generate is the maximum of the sum

The first author has been supported by Coventry University.

The talk at the meeting EACA 2024 has been given by the first author.



FIGURE 1. Piles with a number of grains of wheat growing doubly exponentially

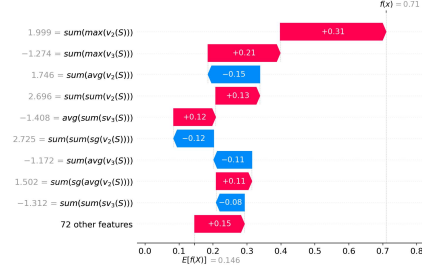


FIGURE 2. An explanation of a decision made by the MLP model to decide whether a given variable ordering was optimal or not.

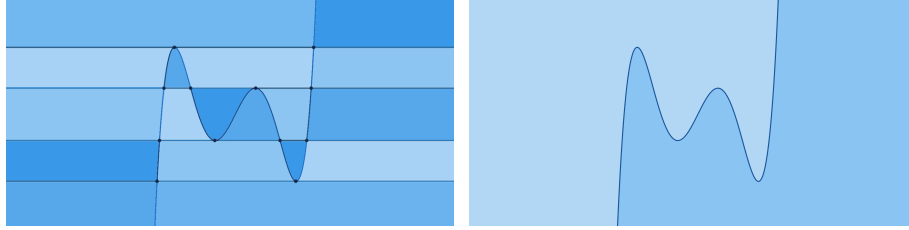


FIGURE 3. CADs sign-invariant for the set of polynomials $\{x^5 + 5x^4 + 5x^3 - 5x^2 - 6x - 2y\}$. Using ordering $x \succ y$, we obtain a CAD with 57 cells (18 shaded areas, 27 curve segments and 12 points). Using the ordering $y \succ x$ generates only 3 cells (2 areas and one curve).

of all the degrees of the variable v_1 inside a polynomial, that is,

$$\text{avg} \left(\text{avg}_{\text{monom} \in p} (\text{degree}_{v_1}(\text{monom})) \right).$$

We denote this feature as $\text{avg}(\text{avg}(v_1(S)))$ and as an example, given $S = \{4v_1^3v_3 - v_2v_3, 2v_1^3v_2 + v_1^2v_2v_3 + 2v_1^2v_3^3 + 7\}$, $\text{avg}(\text{avg}(v_1(S))) = 7$.

27 unique features were generated this way for each variable, adding up to a total of 81 features to describe sets of polynomials in three variables. These features were used to train

USING EXPLAINABLE AI TO EXTRACT INSIGHTS ON ALGEBRAIC PROCEDURES: A CASE STUDY ON VARIABLE ORDE

	KNN	MLP
1	$avg(max(v_3(S)))$	$sum(max(v_3(S)))$
2	$sum(max(v_3(S)))$	$sum(max(v_2(S)))$
3	$avg(max(v_2(S)))$	$sum(avg(v_3(S)))$
4	$sum(max(v_2(S)))$	$avg(sum(sv_3(S)))$
5	$max(max(v_1(S)))$	$sum(avg(v_2(S)))$

	SVM	DT
1	$avg(max(v_1(S)))$	$avg(avg(v_2(S)))$
2	$avg(max(v_2(S)))$	$avg(avg(sg_1(S)))$
3	$sum(max(v_2(S)))$	$max(sum(v_3(S)))$
4	$avg(max(v_3(S)))$	$avg(avg(v_3(S)))$
5	$sum(max(v_3(S)))$	$avg(max(v_1(S)))$

TABLE 1. The top five features that each model found to have the highest average impact on model output magnitude.

various machine learning models: Decision Tree (DT), Random Forest (RF), Multi-Layer Perceptron (MLP) and Support Vector Machine (SVM).

2. EXTRACTING A HEURISTIC USING EXPLAINABLE AI

We introduce the technique employed to measure the impact of each feature in a decision taken by the model, how we aggregated that information to identify the most impactful features overall, and finally how we combine them to create a heuristic.

2.1. SHAP. The SHAP approach was introduced in 2017 by [5] as a unification of existing explanation methods. It is model-agnostic implying that it can be applied to any model and it is a type of post-hoc explainability, that is, it explains an already existing model, it doesn't create models that are intrinsically explainable.

To illustrate the impact that each feature had in a decision made by a model according to SHAP a waterfall plot like that in Figure 2 can be used, in which the features that contribute to a positive response are the red bars and those at the top have the largest effect on the output. In the figure, $sum(max(v_2(S)))$ is the most impactful feature.

2.2. Identifying most impactful features. To find the most impactful features we aggregated the impact of these features across all decisions made by each model, being the most impactful ones those that appear in Table 1.

To combine these classifications into a single one we used a votation system, assigning one to each winner, a half to each second and so on, resulting

2.3. Creating a heuristic. We created a simple heuristic that chose a variable first if it minimised the most impactful feature, breaking ties with the second most impactful, and if there was another tie with the third one it picked randomly. We baptised it as T1 and it outperformed existing heuristics as can be seen in Figure 4.

Feature Name	Voted Score
$sum(max(v_i(S)))$	3.333
$avg(avg(v_i(S)))$	2.167
$sum(sum(v_i(S)))$	1.158
$avg(avg(sg_i(S)))$	1.15
$sum(sg(sum(v_i(S))))$	0.794

TABLE 2. Voted score of merged and aggregated features across all models.

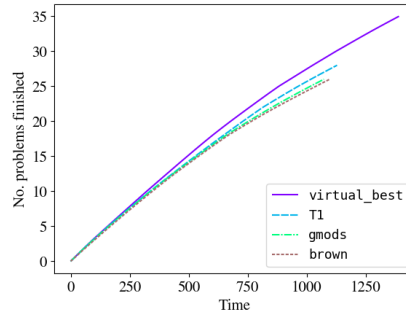


FIGURE 4. Survival plot for best-existing heuristics and new heuristics proposed in the problems that take more than 30 seconds for all the orderings.

REFERENCES

1. Christopher W. Brown and James H. Davenport, *The complexity of quantifier elimination and cylindrical algebraic decomposition*, Proceedings of the International Symposium on Symbolic and Algebraic Computation, ISSAC (2007), 54–60.
2. Tereso del Río and Matthew England, *Data augmentation for mathematical objects*, Proceedings of the 8th Workshop on Satisfiability Checking and Symbolic Computation (SC² 2023) (Erika Ábrahám and Thomas Sturm, eds.), CEUR Workshop Proceedings, no. 3455, 2023, pp. 29–38.
3. Dorian Florescu and Matthew England, *Algorithmically generating new algebraic features of polynomial systems for machine learning*, Proceedings of the 4th Workshop on Satisfiability Checking and Symbolic Computation (SC² 2019) (J. Abbott and A. Griggio, eds.), CEUR Workshop Proceedings, no. 2460, CEUR-WS, 2019.
4. ———, *A machine learning based software pipeline to pick the variable ordering for algorithms with polynomial inputs*, Mathematical Software – ICMS 2020 (A. Bigatti, J. Carette, James H. Davenport, M. Joswig, and T. de Wolff, eds.), Lecture Notes in Computer Science, vol. 12097, Springer International Publishing, 2020, pp. 302–311.
5. Scott M. Lundberg and Su-In Lee, *A unified approach to interpreting model predictions*, Proceedings of the 31st International Conference on Neural Information Processing Systems (2017), 4768–4777.

Coventry University

Email address: delriot@coventry.ac.uk

ASYMMETRIC QUANTUM CODES FROM PROJECTIVE REED-MULLER CODES

DIEGO RUANO AND RODRIGO SAN-JOSÉ

ABSTRACT. We obtain the relative hull of projective Reed-Muller codes over the projective plane by translating the problem to a problem regarding polynomials in a quotient ring. The dimension of the hull determines the minimum number of maximally entangled pairs required for the corresponding entanglement-assisted quantum error-correcting code. Hence, we completely determine the parameters of the asymmetric entanglement-assisted quantum error-correcting codes constructed with projective Reed-Muller codes over the projective plane. Moreover, we also show how to increase the dimension of the hull via monomially equivalent codes in some cases. This allows us to construct quantum codes without requiring entanglement assistance.

INTRODUCTION

Evaluation codes, have a rich algebraic structure and can be studied using tools from commutative algebra [6, 8]. In particular, projective Reed-Muller codes are a family of evaluation codes obtained by evaluating homogeneous polynomials of a given degree at the projective space [7, 12]. From the algebraic point of view, the interest of evaluation codes lies in the fact that they allow us to translate problems concerning applications of coding theory to questions regarding polynomials in a quotient ring.

The importance of quantum error-correcting codes (QECCs) is growing in parallel to the interest in quantum computing, as QECCs are necessary to achieve fault tolerant computation [11] and for quantum communication. One can construct QECCs from self-orthogonal classical linear codes using the CSS construction [3, 13]. However, for entanglement-assisted quantum error-correcting codes (EAQECCs) [2], the self-orthogonality condition is no longer required. We consider the asymmetric case, where the corresponding EAQECCs have two minimum distances δ_z and δ_x , measuring the error-correction capability for phase-shift errors and qudit-flip errors [5], respectively. For the CSS construction, one can consider two codes C_1 and C_2 , and the minimum number required of maximally entangled quantum states is given by $c := \dim C_1 - \dim C_1 \cap C_2^\perp$. Therefore, the dimension of the *relative hull* of C_1 with respect to C_2 , defined in [1] as

$$\text{Hull}_{C_2}(C_1) := C_1 \cap C_2^\perp,$$

Both authors have been partially supported by Grant TED2021-130358B-I00 funded by MCIN/AEI/10.13039/501100011033 and by the “European Union NextGenerationEU/PRTR”, by Grant PID2022-138906NB-C21 funded by MCIN/AEI/10.13039/501100011033 and by ERDF “A way of making Europe”, and QCAYLE project funded by MCIN, the European Union NextGenerationEU (PRTR C17.I1) and Junta de Castilla y León. The second author has also been partially supported by Grant FPU20/01311 funded by the Spanish Ministry of Universities.

The talk at the meeting EACA 2024 has been given by the second author.

determines the parameter c . In this work, we aim to give formulas for the dimension of the relative hull, when the codes considered are projective Reed-Muller codes. We also find conditions to increase the dimension of the hull via monomially equivalent codes, thus decreasing the parameter c .

1. PRELIMINARIES

Let $\mathbb{F}_q$ be the finite field with q elements, and let $\mathbb{P}^m$ be the projective space over $\mathbb{F}_q$. We fix representatives for the points of $\mathbb{P}^m$ as follows: for each point $[Q] \in \mathbb{P}^m$, we choose the representative whose leftmost entry is equal to 1. We will denote by $P^m = \{Q_1, \dots, Q_n\} \subset \mathbb{A}^{m+1}$, with $n = |P^m| = \frac{q^{m+1}-1}{q-1}$, the set of representatives that we have chosen.

We consider now the polynomial ring $S = \mathbb{F}_q[x_0, \dots, x_m]$. The *evaluation map* is the $\mathbb{F}_q$ -linear map defined by

$$\text{ev} : S \rightarrow \mathbb{F}_q^n, \quad f \mapsto (f(Q_1), \dots, f(Q_n)).$$

Let d be a positive integer. If we consider $S_d \subset S$, the set of homogeneous polynomials of degree d , we have that $\text{ev}(S_d)$ is the *projective Reed-Muller code* of degree d , which we will denote by $\text{PRM}_d(m)$. Their parameters were determined in [12], and are summarized in the following result.

Theorem 1.1. *The projective Reed-Muller code $\text{PRM}_d(q, m)$, $1 \leq d \leq m(q-1)$, is an $[n, k]$ -code with*

$$n = \frac{q^{m+1} - 1}{q - 1},$$

$$k = \sum_{t \equiv d \pmod{q-1}, 0 < t \leq d} \left(\sum_{j=0}^{m+1} (-1)^j \binom{m+1}{j} \binom{t-jq+m}{t-jq} \right).$$

For the minimum distance, we have

$$\text{wt}(\text{PRM}_d(q, m)) = (q-s)q^{m-r-1}, \quad \text{where } d-1 = r(q-1) + s, \quad 0 \leq s < q-1.$$

Since $\text{PRM}_d(m) = \text{ev}(S_d)$, we have the isomorphism

$$\text{PRM}_d(m) \cong S_d / (I(P^m) \cap S_d) \cong (S_d + I(P^m)) / I(P^m),$$

where $I(P^m)$ is the vanishing ideal of P^m . This isomorphism allows us to view the vectors of the code as polynomials in a quotient ring. Moreover, we can express many important aspects of the code purely in terms of polynomials, for example the minimum distance [6] or their duals [8]. In what follows, we will abuse the notation and denote $S_d / I(P^m) = (S_d + I(P^m)) / I(P^m)$. Moreover, for a polynomial $f \in S$, we will use the same notation f for both the polynomial and its class in $S / I(P^m)$. The theory of Gröbner bases is one of the main tools that are used for studying evaluation codes using this approach. We introduce now some Gröbner-related results for projective Reed-Muller codes from [4].

Theorem 1.2. *A universal Gröbner basis for $I(P^m)$ is given by the generators*

$$I(P^m) = \langle x_0^2 - x_0, x_1^q - x_1, x_2^q - x_2, \dots, x_m^q - x_m, (x_0 - 1)(x_1^2 - x_1), \\ (x_0 - 1)(x_1 - 1)(x_2^2 - x_2), \dots, (x_0 - 1) \cdots (x_{m-1}^2 - x_{m-1}), (x_0 - 1) \cdots (x_m - 1) \rangle.$$

In this work we will mainly study the case $m = 2$, since we want to obtain explicit formulas and they get increasingly more involved when we increase m . For $m = 2$ we have

$$I(P^2) = \langle x_0^2 - x_0, x_1^q - x_1, x_2^q - x_2, (x_0 - 1)(x_1^2 - x_1), (x_0 - 1)(x_1 - 1)(x_2 - 1) \rangle.$$

Lemma 1.3. *Let $1 \leq d \leq 2(q - 1)$. We consider the following sets of monomials:*

$$\begin{aligned} A_1^d &= \{x_0^{a_0} x_1^{a_1} x_2^{a_2} \mid a_0 > 0, a_0 + a_1 + a_2 = d, 0 \leq a_1, a_2 \leq q - 1\}, \\ A_2^d &= \{x_1^{a_1} x_2^{a_2} \mid a_1 > 0, a_1 + a_2 = d, 0 \leq a_2 \leq q - 1\}, \quad A_3^d = \{x_2^d\}. \end{aligned}$$

Then, $A^d = A_1^d \cup A_2^d \cup A_3^d$ forms a basis for $S_d/I(P^2)$.

2. RELATIVE HULL OF PROJECTIVE REED-MULLER CODES

We start by computing bases for $S_{d_1}/I(P^2) \cap S_{d_2}/I(P^2)$ for any $1 \leq d_1 < d_2 \leq 2(q - 1)$. We do this by considering the bases from Lemma 1.3 for $S_{d_1}/I(P^2)$ and $S_{d_2}/I(P^2)$, and then dividing them by the Gröbner basis from Theorem 1.2, which helps us to discuss which polynomials lie in the intersection. Since, for $d \not\equiv 0 \pmod{q - 1}$, the family of projective Reed-Muller codes is closed under duality [12], the dimension of these vector spaces gives the dimension for the relative hulls of projective Reed-Muller codes.

In the following, for an integer $0 \leq z \leq 2(q - 1)$, we denote by $\bar{z}$ the integer $1 \leq \bar{z} \leq q - 1$ such that $\bar{z} \equiv z \pmod{q - 1}$ if $z > 0$, and $\bar{z} = 0$ if $z = 0$.

Theorem 2.1. *Let $1 \leq d_1 < d_2 \leq 2(q - 1)$, and let $Y = \{0, 1, \dots, \min\{d_1 - 1, d_2 - q\}\}$. If $d_1 \equiv d_2 \pmod{q - 1}$, A^{d_1} is a basis for $S_{d_1}/I(P^2) \cap S_{d_2}/I(P^2)$. If $d_1 \not\equiv d_2 \pmod{q - 1}$, the following set B is a basis for $S_{d_1}/I(P^2) \cap S_{d_2}/I(P^2)$:*

$$B = \begin{cases} A_1^{d_1} & \text{if } d_2 \leq q - 1, \\ A_1^{d_1} \cup \left(\bigcup_{a_2 \in Y} \{x_1^{d_1 - a_2} x_2^{a_2}\} \right) & \text{if } d_1 \leq q - 1 < d_2, \\ A_1^{d_1} \cup \left(\bigcup_{a_2 \in Y} \{x_1^{d_1 - a_2} x_2^{a_2}\} \right) \cup \{Q_{d_1, d_2}\} & \text{if } q \leq d_1, \end{cases}$$

where

$$Q_{d_1, d_2} := x_2^{d_1} + x_1^{d_1 - \bar{d}_2} x_2^{\bar{d}_2} + x_0^{d_1 - \bar{d}_2} x_2^{\bar{d}_2} + x_0^{d_1 - \bar{d}_2} x_1^{\bar{d}_2 - \bar{d}_1} x_2^{\bar{d}_1} \in S_{d_1}.$$

In particular, the image by the evaluation map of B is a basis for $\text{PRM}_{d_1}(2) \cap \text{PRM}_{d_2}(2)$.

Using this result about the relative hull, and the CSS construction that we introduce next in Theorem 2.2, we can give the parameters of the asymmetric EAQECs arising from projective Reed-Muller codes in Theorem 2.3.

Theorem 2.2. *Let $C_i \subset \mathbb{F}_q^n$ be linear codes of dimension k_i , for $i = 1, 2$. Then, there is an asymmetric EAQEC with parameters $[[n, \kappa, \delta_z/\delta_x; c]]_q$, where*

$$\begin{aligned} c &= k_1 - \dim(C_1 \cap C_2^\perp), \quad \kappa = n - (k_1 + k_2) + c, \\ \delta_z &= \text{wt}\left(C_1^\perp \setminus (C_1^\perp \cap C_2)\right) \quad \text{and} \quad \delta_x = \text{wt}\left(C_2^\perp \setminus (C_2^\perp \cap C_1)\right). \end{aligned}$$

Theorem 2.3. *Let $1 \leq d_1 \leq d_2 < 2(q - 1)$, $d_1 + d_2 \not\equiv 0 \pmod{q - 1}$, $d_1 \neq q - 1 \neq d_2$. Let $k_1 = |A_1^{d_1}|$ and $k_2 = |A_1^{d_2^\perp}|$, where $d_2^\perp = 2(q - 1) - d_2$. Then we can construct an asymmetric EAQEC with parameters $[[n, \kappa, \delta_z/\delta_x; c]]_q$, where $n = q^2 + q + 1$, $\kappa = n - (\dim \text{PRM}_{d_1}(2) + \dim \text{PRM}_{d_2}(2)) + c$, $\delta_z = \text{wt}(\text{PRM}_{d_2}^\perp(2))$, $\delta_x = \text{wt}(\text{PRM}_{d_1}^\perp(2))$, and the value of c is:*

(1) If $d_1 + d_2 < 2(q - 1)$:

$$c = \begin{cases} d_1 + 1 - \min\{d_1, q - 1 - d_2\} & \text{if } d_2 < q - 1, \\ d_1 + 1 & \text{if } q \leq d_2. \end{cases}$$

(2) If $d_1 + d_2 > 2(q - 1)$:

$$c = \begin{cases} k_1 - k_2 + d_1 + 1 & \text{if } d_1 < q - 1, \\ k_1 - k_2 + q + 1 - \min\{d_2^\perp, d_1 - (q - 1)\} & \text{if } q \leq d_1. \end{cases}$$

For the general case over $\mathbb{P}^m$, we can find conditions to increase the dimension of the relative hull. This allows us to construct QECCs without requiring entanglement assistance, which are less expensive to implement.

Theorem 2.4. *Let $1 \leq d_1 \leq d_2 < q - 2$ such that $d_1 + d_2 < q - 2$. Then we can construct a quantum code with parameters $[[n, \kappa, \delta_z/\delta_x]]_q$, where $n = \frac{q^{m+1}-1}{q-1}$, $\kappa = n - (\dim \text{PRM}_{d_1}(m) + \dim \text{PRM}_{d_2}(m))$, $\delta_z = \text{wt}(\text{PRM}_{d_2}^\perp(m))$ and $\delta_x = \text{wt}(\text{PRM}_{d_1}^\perp(m))$.*

As seen in [9, 10], some of these results can be generalized to the Hermitian hull and the corresponding quantum codes obtained with the Hermitian construction.

REFERENCES

- [1] S. E. Anderson, E. Camps-Moreno, H. H. López, G. L. Matthews, D. Ruano, and I. Soprunov. Relative hulls and quantum codes. *IEEE Trans. Inform. Theory*, 70(5):3190–3201, 2024.
- [2] T. Brun, I. Devetak, and M.-H. Hsieh. Correcting quantum errors with entanglement. *Science*, 314(5798):436–439, 2006.
- [3] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane. Quantum error correction via codes over $\text{GF}(4)$. *IEEE Trans. Inform. Theory*, 44(4):1369–1387, 1998.
- [4] P. Gimenez, D. Ruano, and R. San-José. Subfield subcodes of projective Reed-Muller codes. *Finite Fields Appl.*, 94, 102353, 2024.
- [5] L. Ioffe and M. Mézard. Asymmetric quantum error-correcting codes. *Phys. Rev. A*, 75:032345, Mar 2007.
- [6] D. Jaramillo, M. Vaz Pinto, and R. H. Villarreal. Evaluation codes and their basic parameters. *Des. Codes Cryptogr.*, 89(2):269–300, 2021.
- [7] G. Lachaud. The parameters of projective Reed-Muller codes. *Discrete Math.*, 81(2):217–221, 1990.
- [8] H. H. López, I. Soprunov, and R. H. Villarreal. The dual of an evaluation code. *Des. Codes Cryptogr.*, 89(7):1367–1403, 2021.
- [9] D. Ruano and R. San-José. Hulls of projective Reed-Muller codes over the projective plane. *ArXiv 2312.13921*, 2023.
- [10] D. Ruano and R. San-José. The hull variation problem for projective Reed-Muller codes and quantum error-correcting codes. *ArXiv 2312.15308*, 2023.
- [11] P. Shor. Fault-tolerant quantum computation. In *Proceedings of 37th Conference on Foundations of Computer Science*, pages 56–65, 1996.
- [12] A. B. Sørensen. Projective Reed-Muller codes. *IEEE Trans. Inform. Theory*, 37(6):1567–1576, 1991.
- [13] A. M. Steane. Simple quantum error-correcting codes. *Phys. Rev. A* (3), 54(6):4741–4751, 1996.

University of Valladolid

Email address: `diego.ruano@uva.es`

University of Valladolid

Email address: `rodrigo.san-jose@uva.es`

BASES DE SAITO PARA UNA CURVA CON UN PAR DE PUISEUX

DAVID SENOVILLA-SANZ

RESUMEN. Given C a germ of an holomorphic plane curve in $(\mathbb{C}^2, 0)$ and with one Puiseux pair, we present a new approach on the computation of a basis of the module of holomorphic 1-forms with C as an invariant curve.

INTRODUCCIÓN

Dado C un germen de curva plana holomorfa en $(\mathbb{C}^2, 0)$, esta viene definida por una ecuación local $f = 0$, con $f \in \mathbb{C}\{x, y\}$ una serie de potencias convergente con coeficientes complejos. Denotamos por $\Omega_{\mathbb{C}^2, 0}$ el $\mathbb{C}\{x, y\}$ -módulo de 1-formas diferenciales de $\mathbb{C}^2$ en el origen. Decimos que $\omega \in \Omega_{\mathbb{C}^2, 0}$ tiene la curva C *invariante* si $\omega \wedge df = fgdx \wedge dy$ con $g \in \mathbb{C}\{x, y\}$.

Consideramos el submódulo $\Omega_{\mathbb{C}^2, 0}[C] \subset \Omega_{\mathbb{C}^2, 0}$ de 1-formas holomorfas que tienen a C como curva invariante, en [8] se mostró que se trata de un $\mathbb{C}\{x, y\}$ -módulo libre de rango 2, una base de $\Omega_{\mathbb{C}^2, 0}[C]$ recibe el nombre de *base de Saito* de la curva C .

Para una 1-forma $\omega = Adx + Bdy$, denotamos su multiplicidad en el origen como $\text{mult}_0(\omega) = \min\{\text{mult}_0(A), \text{mult}_0(B)\}$. De entre todas las bases de Saito $\{\eta_1, \eta_2\}$ de C , podemos considerar aquellas cuyo par de multiplicidades $(\nu_1, \nu_2) = (\text{mult}_0(\eta_1), \text{mult}_0(\eta_2))$ cumple que $\nu_1 + \nu_2$ es máximo respecto de todas las posibles bases de Saito de C . Llamaremos *par de multiplicidades maximales* de la curva C al par (ν_1, ν_2) . Se tiene que el par de multiplicidades maximales de una curva es, salvo permutación, un *invariante analítico* de esta, es decir, no varía por cambio de coordenadas holomorfo, ver [4]. Además siempre se tiene que $\nu_1 + \nu_2 \leq \text{mult}_0(f)$.

Presentamos aquí un método que permite calcular una base de Saito de la curva C cuando esta es irreducible y, además tiene un par de Puiseux. Este está basado en el uso de otros invariantes analíticos de la curva. En particular, se apoya en el denominado semimódulo de valores diferenciales de C , ver [3].

1. SEMIMÓDULO DE VALORES DIFERENCIALES

Sea C un germen de una curva plana holomorfa irreducible en $(\mathbb{C}^2, 0)$. Por el Teorema de Newton-Puiseux, existe una parametrización *primitiva* de la curva de la forma:

$$\phi(t) = (x(t), y(t)); \quad \text{mult}_0(C) = \min\{\text{ord}_t(x(t)), \text{ord}_t(y(t))\} = n.$$

El autor ha sido parcialmente financiado por los proyectos españoles PID2019-105621GB-I00 y PID2022-139631NB-I00; y por la beca predoctoral "Concepción Arenal" de la Universidad de Cantabria y del Gobierno de Cantabria.

Si además suponemos que nos encontramos en coordenadas adaptadas a C , podemos escribir la parametrización de la siguiente forma:

$$\phi(t) = (t^n, at^m + h.o.t.); \quad a \neq 0, m > n \text{ y } n \nmid m.$$

Si $\gcd(n, m) = 1$ y $n \geq 2$, decimos que C tiene un *par de Puiseux* (n, m) . Esto es equivalente a que el *semigrupo* de C sea $\Gamma = \langle n, m \rangle$. Recordamos que el semigrupo de una curva se define como

$$\Gamma = \{\text{ord}_t(h \circ \phi) : h \in \mathbb{C}\{x, y\}\}.$$

De forma similar podemos definir el *semimódulo de valores diferenciales* de C como

$$\Lambda = \{\nu_C(\omega) : \omega \in \Omega_{\mathbb{C}^2, 0}\}.$$

Donde $\nu_C(\omega) := \text{ord}_t(\alpha(t)) + 1$, $\phi^*(\omega) = \alpha(t)dt$, y $\phi^*(\omega)$ es el pullback de la 1-forma ω por $\phi(t)$. Es decir, si escribimos $\omega = A(x, y)dx + B(x, y)dy$, tenemos que

$$\phi^*(\omega) = (A(x(t), y(t))x'(t) + B(x(t), y(t))y'(t))dt,$$

con $x'(t), y'(t)$ las derivadas de $x(t)$ e $y(t)$. Se tiene que el semimódulo de valores diferenciales de una curva es un invariante analítico de esta.

Se cumple que Λ tiene estructura de Γ -*semimódulo*, o lo que es equivalente, para todo $\gamma \in \Gamma$, $\lambda \in \Lambda$, se tiene que $\lambda + \gamma \in \Lambda$.

Por ser Λ un Γ -semimódulo, existe una única sucesión creciente de elementos de Λ , $(\lambda_{-1}, \lambda_0, \dots, \lambda_s)$, donde s es minimal con la propiedad de que

$$\Lambda = \bigcup_{i=-1}^s (\lambda_i + \Gamma).$$

La sucesión $(\lambda_{-1}, \lambda_0, \dots, \lambda_s)$ recibe el nombre de *base* del semimódulo y el índice s se denomina la *longitud* de Λ . Para el conjunto de valores diferenciales se cumple siempre que $\lambda_{-1} = n$ y $\lambda_0 = m$. Llamamos *base estándar minimal* del módulo de formas diferenciales de C a una sucesión de 1-formas $(\omega_{-1}, \omega_0, \dots, \omega_s)$ tales que $\nu_C(\omega_i) = \lambda_i$ para $-1 \leq i \leq s$.

Para $-1 \leq j \leq s$, denotamos por $\Lambda_j = \bigcup_{i=-1}^j (\lambda_i + \Gamma)$. A partir de ahora supondremos que C tiene un par de Puiseux (n, m) , es decir $\Gamma = \langle n, m \rangle$. Podemos definir los *ejes*: u_j^n, u_j^m, u_j y $\tilde{u}_j$ con $1 \leq j \leq s+1$, de la siguiente manera

- $u_j^n = \min\{\lambda_{j-1} + n\ell \in \Lambda_{j-2} : \ell > 0\}.$
- $u_j^m = \min\{\lambda_{j-1} + m\ell \in \Lambda_{j-2} : \ell > 0\}.$
- $u_j = \min\{u_j^n, u_j^m\}$ y $\tilde{u}_j = \max\{u_j^n, u_j^m\}.$

De forma similar describimos los *valores críticos*: t_j^n, t_j^m, t_j y $\tilde{t}_j$ con $1 \leq j \leq s+1$ como

- $t_j^* = t_{j-1} + (u_j^* - \lambda_{j-1})$, con $*$ = n, m y $t_0 = \lambda_0$.
- $t_j = \min\{t_j^n, t_j^m\}$ y $\tilde{t}_j = \max\{t_j^n, t_j^m\}.$

2. SOBRE LAS BASES DE SAITO

Fijado un par (n, m) con $2 \leq n < m$ con $\gcd(n, m) = 1$. Dada una función $h \in \mathbb{C}\{x, y\}$, la escribimos de la siguiente forma:

$$h = \sum_{\alpha, \beta \geq 0} h_{\alpha\beta} x^\alpha y^\beta.$$

Definimos el *valor monomial* de h respecto de n y m como

$$\nu_{n,m}(h) := \min\{n\alpha + m\beta : h_{\alpha\beta} \neq 0\}.$$

Si ahora tenemos $\omega = Adx + Bdy \in \Omega_{\mathbb{C}^2,0}$, entonces definimos su *valor monomial* como $\nu_{n,m}(\omega) = \min\{\nu_{n,m}(xA), \nu_{n,m}(yB)\}$.

Teorema 2.1. *Sea C una curva con un par de Puiseux (n, m) , y supongamos que nos encontramos en coordenadas adaptadas respecto de C , entonces podemos encontrar 1-formas ω_{s+1} y $\tilde{\omega}_{s+1}$ tales que:*

1. ω_{s+1} y $\tilde{\omega}_{s+1}$ tienen a C como curva invariante.
2. $\nu_{n,m}(\omega_{s+1}) = t_{s+1}$ y $\nu_{n,m}(\tilde{\omega}_{s+1}) = \tilde{t}_{s+1}$.

Teorema 2.2. *Las 1-formas $\{\omega_{s+1}, \tilde{\omega}_{s+1}\}$ son una base de Saito de la curva C .*

El cálculo aproximado de las 1-formas $\omega_{s+1}, \tilde{\omega}_{s+1}$ se basa en el algoritmo de Büchberger empleado para obtener una base estándar minimal $(\omega_{-1}, \omega_0, \dots, \omega_s)$, ver [6]. Decimos aproximado, pues el método solo nos permite obtener una aproximación de los coeficientes de las 1-formas como serie de potencias formales hasta cualquier orden prefijado.

Procedemos a explicar cómo se calcula una 1-forma que tiene a C invariante y con valor monomial t_{s+1}^n que recordemos que puede ser t_{s+1} o $\tilde{t}_{s+1}$. Para t_{s+1}^m se procedería de forma similar.

Notamos que existe un único índice $-1 \leq k \leq s-1$ tal que $u_{s+1}^n = \lambda_s + n\ell = \lambda_k + mb$. Escribimos $\eta = x^\ell \omega_s + \mu y^b \omega_k$, donde $\mu \in \mathbb{C}^*$ es la única constante no nula tal que

$$\nu_C(\eta) > \nu_C(x^\ell \omega_s) = \nu_C(y^b \omega_k) = u_{s+1}^n.$$

Si $\nu_C(\eta) = \infty$ entonces C es invariante y, en este caso hemos terminado, pues se cumple que $\nu_{n,m}(\eta) = t_{s+1}^n$. Si $\nu_C(\eta) = \lambda < \infty$, por definición de base de un semimódulo, podemos escribir $\lambda = \lambda_i + n\alpha + m\beta$ para algún $-1 \leq i \leq s$. Ponemos

$$\eta' = \eta + \mu' x^\alpha y^\beta \omega_i,$$

donde de nuevo μ' es la única constante no nula tal que $\nu_C(\eta') > \nu_C(\eta) = \nu_C(x^\alpha y^\beta \omega_i)$. Al igual que antes se sigue teniendo que $\nu_{n,m}(\eta') = t_{s+1}^n$. Iterando este procedimiento se obtiene una 1-forma con el valor monomial t_{s+1}^n y la curva C invariante.

Debido a que en general este método puede que no finalice en un número finito de pasos, no está claro que el objeto $\hat{\omega}$ que se retorna en el límite sea holomorfo o no. Actualmente no se conocen condiciones que garanticen que el método retorne 1-formas holomorfas, ni tampoco se sabe si existen casos que en los que se retornen 1-formas no convergentes. No obstante, aún suponiendo que se obtiene un objeto no holomorfo, por el Teorema de Aproximación de Artin, ver [1], sabemos que existe una 1-forma holomorfa tan próxima como deseemos a $\hat{\omega}$ con C invariante y el valor monomial deseado. En este caso, la noción de proximidad viene dada por la topología $\mathfrak{m}$ -ádica de $\mathbb{C}\{x, y\}$ con $\mathfrak{m} = (x, y)$.

Sabiendo cómo se pueden calcular 1-formas ω_{s+1} y $\tilde{\omega}_{s+1}$ es posible contruir el siguiente ejemplo.

Ejemplo 2.3. Consideremos la curva C_1 dada por la parametrización

$$\phi_1(t) = (t^7, t^{36} + t^{116} + 28/9t^{196} + h.o.t.),$$

y la curva C_2 dada por

$$\phi_2(t) = (t^7, t^{36} + t^{116} - 4/171t^{131} + 1/1782t^{146} - 1/72900t^{161} + h.o.t.).$$

Ambas curvas tienen el mismo conjunto de valores diferenciales dados por la base $(7, 36, 123)$. No obstante, se tiene que el par de multiplicidades maximales dadas por sus bases de Saito son $(3, 4)$ y $(2, 5)$ respectivamente. Esto muestra que fijar el semimódulo de valores diferenciales de la curva, no determina el par de multiplicidades.

Para determinar los pares de multiplicidades maximales calculamos, usando el método anterior, una base de Saito para C_1 y otra para C_2 . En el caso de C_1 obtenemos la base dada por

$$\omega_2 = 36x^3(7xdy - 36ydx) - 560y^3dy; \quad \tilde{\omega}_2 = y^3(7xdy - 36ydx) - 80x^{32}dx + \dots$$

En cuanto a la curva C_2 obtenemos, por el método anterior, la siguiente base

$$\omega'_2 = (36x^3 + y)(7xdy - 36ydx) - 560y^3dy; \quad \tilde{\omega}'_2 = y^3(7xdy - 36ydx) - 80x^{32}dx + \dots$$

Donde en ambos casos los puntos suspensivos denotan términos de mayor valor diferencial que $\nu_C(x^{32}dx) = 231$. Notamos que la base de Saito de C_1 calculada nos da directamente el par de multiplicidades maximales de C_1 . Recuérdese que la suma de los elementos del par de multiplicidades maximales siempre está acotada superiormente por la multiplicidad en el origen de la curva, en este caso 7.

Por el contrario, la base de Saito calculada para C_2 no da su par de multiplicidades maximales. Para encontrar el par de multiplicidades maximales $(2, 5)$ tomamos base de Saito $\{\omega'_2, \tilde{\omega}'_2 - y^2\omega'_2\}$ de C_2 .

REFERENCIAS

- [1] M. Artin, *On the Solutions of Analytic Equations*, Invent. Math., **5**, (1968), 277–291.
- [2] F. Cano, N. Corral, and D. Senovilla-Sanz, *Analytic semiroots for plane branches and singular foliations*, Bull. Braz. Math. Soc. (N.S.), **54**(2), (2023), Paper No. 27, 49 pp.
- [3] F. Cano, N. Corral, and D. Senovilla-Sanz, *Computing a Saito basis from a standard basis*, arXiv:2404.00316.
- [4] Y. Genzmer, *Dimension of the Moduli Space of a Germ of Curve in $\mathbb{C}^2$* , Int. Math. Res. Not. IMRN, **5**, (2022), 3805–3859.
- [5] C. Delorme, *Sur les modules des singularités de courbes planes*, Bull. Soc. Math. France, **106**, (1978), 417–446.
- [6] A. Hefez, M. E. Hernandez, *Computational methods in the local theory of curves*, Publicações Matemáticas do IMPA, [IMPA Mathematical Publications] 23o Colóquio Brasileiro de Matemática. Instituto de Matemática Pura e Aplicada (IMPA), Rio de Janeiro, (2001).
- [7] A. Hefez, M. E. Hernandez, *The analytic classification of plane branches*, Bull. Lond. Math. Soc., **43**(2), (2011), 289–298.
- [8] K. Saito, *Theory of logarithmic differential forms and logarithmic vector fields*, J. Fac. Sci. Univ. Tokyo Sect. IA Math, **27**(2), (1980), 265–291.
- [9] C.T.C Wall, *Singular points of plane curves*, 63, Cambridge University Press, (2004).
- [10] O. Zariski, *The moduli problem for plane branches. With an appendix by Bernard Teissier*, Translated from the 1973 French original by Ben Lichtin, University Lecture Series, 39, American Mathematical Society, Providence, RI, (2006).

Departamento de Matemáticas, Estadística y Computación, Universidad de Cantabria, Avda. de los Castros s/n, 39005 Santander, Spain.

Email address: david.senovilla@unican.es

Posters

Encuentro de Álgebra computacional y aplicaciones

San Lorenzo, Junio de 2024 Poster abstract

Toric Sylvester forms

Carles Checa^{*}

Laurent Busé[†]

The elimination of variables from a system of homogeneous polynomials is deeply connected to the saturation of ideals with respect to a certain geometrically irrelevant ideal. Thus, the search and study of universal generators of the saturation of an ideal generated by generic homogeneous polynomials, such as Jacobian determinants, is an important topic in elimination theory. We investigate this question in the general setting of homogeneous polynomials in the Cox ring of a projective toric variety X_Σ . As our main results, we establish a duality property and then we make it explicit by introducing toric Sylvester forms, under a certain positivity assumption on X_Σ . In particular, we prove that toric Sylvester forms yield a basis of the graded piece at $\alpha \in \text{Pic}(X_\Sigma)$ of I^{sat}/I , where I denotes an ideal generated by $n + 1$ generic forms, n is the dimension of X_Σ and I^{sat} the saturation of I with respect to the irrelevant ideal of the Cox ring of X_Σ [4, 3]. These results generalize classical results of Jouanolou in the case where X_Σ is a projective space [6], as well as their extension to the case of a product of projective spaces by Buse-Charadin-Nemati [1]. Then, to illustrate the relevance of toric Sylvester forms we provide some consequences in elimination theory. First, we define hybrid elimination matrices by incorporating toric Sylvester forms in the classical Macaulay matrices; more generally, from the classical Koszul complex we obtain a new complex whose determinant of some of its graded pieces is proved to be equal to the toric resultant in the fashion of Cattani-Dickenstein-Sturmfels for the Jacobian case [2]. Second, we extend the construction of hybrid elimination matrices to the case of overdetermined polynomial systems, providing this way a new family of matrices that can be used for solving such polynomial systems by means of linear algebra methods. Finally, we explore the possibility of using toric Sylvester forms for computing toric

residues of product of forms; this is a generalization of a formula due to Jouanolou in the case X_Σ is a projective space [6, 5].

Acknowledgments The authors received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 860843. They are grateful to Matías R. Bender, Marc Chardin and Carlos D'Andrea for interesting discussions. They also thank Ioannis Z. Emiris, Christos Konaxis and Elias Tsigaridas for their support as advisors of the second author.

References

- [1] Laurent Busé, Marc Chardin, and Navid Nemati. "Multigraded Sylvester forms, duality and elimination matrices". In: *Journal of Algebra* 609 (2022), pp. 514–546. ISSN: 0021-8693. DOI: <https://doi.org/10.1016/j.jalgebra.2022.06.022>.
- [2] Eduardo Cattani, Alicia Dickenstein, and Bernd Sturmfels. "Residues and resultants". In: *Journal of Mathematical Sciences* 5 (1997), pp. 119–148.
- [3] David A. Cox. "The homogeneous coordinate ring of a toric variety". In: *Journal of Algebraic Geometry* 4 (1995), pp. 17–50.
- [4] David A. Cox, John B. Little, and Hal Schenck. *Toric Varieties*. Vol. 114. 3, 2012, pp. 367–380. DOI: <https://doi.org/10.1365/s13291-012-0048-9>.
- [5] Carlos D'Andrea and Amit Khetan. "Macaulay style formulas for toric residues". In: *Compositio Mathematica* 141.3 (2005), pp. 713–728. DOI: [10.1112/S0010437X05001326](https://doi.org/10.1112/S0010437X05001326).
- [6] Jean-Pierre Jouanolou. "Formes d'inertie et résultant: Un formulaire". In: *Advances in Mathematics* 126 (Mar. 1997), pp. 119–250. DOI: [10.1006/aima.1996.1609](https://doi.org/10.1006/aima.1996.1609).

^{*}National and Kapodistrian University of Athens, Athena RC, Greece. Email: cchecha@di.uoa.gr

[†]INRIA Sophia-Antipolis, Université Côte d'Azur. Email: Laurent.Buse@inria.fr

DME⁽⁻⁾-SIGN: A NEW DME CRYPTOSYSTEM FOR SIGNATURES

IGNACIO LUENGO, MARTÍN AVENDAÑO, AND PILAR COSCOJUELA

ABSTRACT. The *DME* cryptosystem is a multivariate post-quantum scheme whose security rely on solving a system of polynomial equations of large degree over a finite field of size $q = 2^n$, where n is a fixed natural number (usually $n = 64, 96, 128$). The scheme is obtained by a composition of n -th rounds, each comprising an exponential map and a linear map. Consequently, the private key is the set of exponential and linear matrices, while the public key are eight polynomials in $\mathbb{F}_q[x_1, \dots, x_8]$. A structural attack to the version **1** submitted to the NIST call in 2023, which had three rounds, was found in **2**. In this poster, we introduce a new version that differs from the previous in two significant facets. Firstly, it has an additional round which increase the number of monomials in the public key. Secondly, only a selectively chosen half of the public key is made public. As a result, the scheme is no longer injective and thus only suitable for digital signature. On the other hand, we present a version for Key Encapsulation Mechanism (KEM), achieved by adding some new polynomials that share support with those derived from the computation of the public key.

In the section called Configuration matrices, we give some details related to the construction of exponential matrices endowed with the desired properties to get an efficient scheme. A notable feature resides in the configuration of exponential matrices, which are 4×4 with at most two non-zero entries of the form 2^α with $\alpha \in [0, \dots, n-1]$ on each row. Furthermore, the linear maps are 8×8 with a 2×2 block structure. Finally, we provide the timings we get for a specific instance of the *DME⁽⁻⁾-Sign*.

REFERENCES

- [1] I. Luengo, M. Avendaño, Pilar Coscojuela (2023). DME: a full encryption, signature and KEM multivariate public key cryptosystem. International Conference on Post-Quantum Cryptography. Springer, 379-402.
- [2] P. Briaud, M. Bros, R. Perlner, D. Smith-Tone (2024). Practical Attack on All Parameters of the DME Signature Scheme. Cryptology ePrint Archive.

Universidad Complutense de Madrid
Email address: `iluengo@ucm.es`

Universidad Complutense de Madrid
Email address: `mavend01@ucm.es`

Universidad Complutense de Madrid
Email address: `picoscoj@ucm.es`

ANALYSIS OF THE CRYSTALS-KYBER IMPLEMENTATION

DIEGO ROJAS RODRÍGUEZ AND LUIS HERNÁNDEZ ENCINAS

ABSTRACT. In this work, we analyze the reference implementation of the post-quantum cryptographic proposal, CRYSTALS-Kyber, which is the only KEM selected by NIST as an standard. We pointing out the main differences between the theoretical algorithms that are part of CRYSTALS-Kyber and its reference implementation.

INTRODUCTION

CRYSTALS-Kyber (or just Kyber) is a lattice-based KEM (Key Encapsulation Mechanism) whose security relies on the hardness of the Ring Learning With Errors (RLWE) problem [2]. RLWE is a version of the Learning With Errors (LWE) problem defined on the polynomial ring $R_q = \mathbb{Z}_q[x]/\langle x^n + 1 \rangle$, where $n \leq 256$ is the polynomial degree and $q = 3329 = 13 \cdot 2^8 + 1$ is a prime number.

1. MAIN PROPERTIES OF KYBER IMPLEMENTATION

Kyber is composed by two main primitives: a Public Key Encryption (PKE) with its corresponding key generation, cipher and decipher algorithms, and a set of functions that conform the KEM via the Fujisaki-Okamoto transform [1] resulting key generation, encapsulation, and decapsulation algorithms. Additionally, PKE uses several functions, among which we highlight Compress (and Decompress) and NTT (Number Theoretic Transform). The reference implementation in Kyber's proposal was done in language C (<https://github.com/pqcrystals/kyber>). This decision might be motivated due to C is the fastest programming language when coding at a low level, even though it may carry some side effects given the lack of native operations for dealing with polynomials in C. This can be seen in the `poly.h` file, where polynomials are defined as 256 indexes of type `int16_t`, integers with sign represented in two's complement (C2) in range $[-2^{15}, 2^{15} - 1]$. Each number in this array represents a coefficient of a polynomial of degree between 0 and 255.

The functions Compress and Decompress are defined as follows:

$$\text{Compress}_q(x, d) = \frac{2^d}{q}x \mod 2^d, \quad \text{Decompress}_q(x, d) = \frac{q}{2^d}x \mod q,$$

where q is the prime used in the definition of the ring R_q , d is an integer parameter determined by the security of Kyber's implementation and x is the coefficient to be compressed.

El segundo autor ha sido parcialmente financiado por la Agencia Estatal de Investigación (AEI) del Ministerio de Ciencia e Innovación (MCIN), proyecto P2QProMeTe (PID2020-112586RB-I00/AEI/10.13039/501100011033), cofinanciado por el Fondo Europeo de Desarrollo Regional (FSE, FEDER y FEDER, UE).

La ponencia en el Encuentro EACA 2024 ha sido presentada por el primer autor.

Both functions aim to discard some bits of the keys whose influence is negligible, and thus shortening key size and as they have similar properties, we will focus just on the Compress function. Some operations, not defined natively in C, needed to be adapted giving raise to the following disparities: 1) The function compresses all coefficients of the polynomial instead of doing it individually. 2) Each signed polynomial coefficient is mapped to its positive representative in pure binary, done efficiently performing the C2 operation to the negative numbers. This is not a native operation to C (see Figure 1a). Moreover, u is shifted 15 times to the right, leaving just its sign bit added to the original number. Finally, the variable is casted to the `uint_t` type, pure binary. 3) Multiplication by 2^d is efficiently performed by arithmetically shifting to the left $d = 4$ times. 4) Moreover, $q/2(\text{Kyber_Q}/2)$ is added and later divided by q . This is an integer division that will return the quotient without decimal part. 5) The resulting number is then operated with an AND (&) with the number 15 (=1111 in pure binary). The value 15 will just leave the 4 least representative bits and discard the rest, equivalent to performing the mod 24 operation. The result after performing one iteration of the loop is equivalent to the function:

$$\text{poly_compress}(x, d) = |x| \frac{2^d}{q} + \frac{q}{2} \mod 2^d.$$

```

void poly_compress(uint8_t r[KYBER_POLYCOMPRESSEDBYTES], const poly *a)
{
    unsigned int i, j;
    int16_t u;
    uint8_t t[8];

    #if (KYBER_POLYCOMPRESSEDBYTES == 128)
        for(i=0; i<KYBER_N/8; i++) {
            for(j=0; j<8; j++) {
                // map to positive standard representatives
                u = a->coeffs[8*i+j];
                u += (u >> 15) & KYBER_Q; //S1 u < 0 => u += 1
                t[j] = (((uint16_t)u << 4) + KYBER_Q/2)/KYBER_Q & 15;
            }

            r[0] = t[0] | (t[1] << 4);
            r[1] = t[2] | (t[3] << 4);
            r[2] = t[4] | (t[5] << 4);
            r[3] = t[6] | (t[7] << 4);
            r += 4;
        }
    #elif (KYBER_POLYCOMPRESSEDBYTES == 160)
        for(i=0; i<KYBER_N/8; i++) {
            for(j=0; j<8; j++) {
                // map to positive standard representatives
                u = a->coeffs[8*i+j];
                u += (u >> 15) & KYBER_Q;
                t[j] = (((uint32_t)u << 5) + KYBER_Q/2)/KYBER_Q & 31;
            }

            r[0] = (t[0] >> 0) | (t[1] << 5);
            r[1] = (t[1] >> 3) | (t[2] << 2) | (t[3] << 7);
            r[2] = (t[3] >> 1) | (t[4] << 4);
            r[3] = (t[4] >> 4) | (t[5] << 1) | (t[6] << 6);
            r[4] = (t[6] >> 2) | (t[7] << 3);
            r += 5;
        }
    #else
        #error "KYBER_POLYCOMPRESSEDBYTES needs to be in {128, 160}"
    #endif
}

```

```

void ntt(int16_t r[256]) {
    unsigned int len, start, j, k;
    int16_t t, zeta;

    k = 1;
    for(len = 128; len >= 2; len >= 1) {
        for(start = 0; start < 256; start = j + len) {
            zeta = zetas[k++];
            for(j = start; j < start + len; j++) {
                t = fgmul(zeta, r[j + len]);
                r[j + len] = r[j] - t;
                r[j] = r[j] + t;
            }
        }
    }
}

```

FIGURE 1. Codes of a) `poly_compress` for Kyber 512, b) the NTT implementation

In addition, it is known that an essential operation and one of the most time consuming for the RLWE problem is the polynomial multiplication over R_q . To improve its efficiency the NTT is used. To multiply two polynomials over R_q they are transformed to the NTT domain, then operated and finally transformed back to the original domain.

We have $x^{256} + 1 = \prod_{i=0}^{127} x^2 - \zeta^{2i+1} = \prod_{i=0}^{127} x^2 - \zeta^{2br7(i)+1}$, where each ζ^i represents a 256-th root of unity and br (bit-reversal) is an operation that inverts the order of the bits in the

binary representation of the number. In a nutshell, $\text{NTT}: R_q \rightarrow R_q$ is defined as a bijection over R_q , so that, if $f \in R_q$, then $\text{NTT}(f) = \hat{f} = \hat{f}_0 + \hat{f}_1x + \dots + \hat{f}_{255}x^{255}$, where

$$\hat{f}_{2i} = \sum_{j=0}^{127} f_{2j} \zeta^{(2br(i)+1)j}, \quad \hat{f}_{2i+1} = \sum_{j=0}^{127} f_{2j+1} \zeta^{(2br(i)+1)j}.$$

Therefore, the algebraic expression of $\hat{f}$ can be reordered as a vector of 128 polynomials of degree 1: $\hat{f} = (\hat{f}_0 + \hat{f}_1x, \hat{f}_2 + \hat{f}_3x, \dots, \hat{f}_{244} + \hat{f}_{255}x^{255})$. Using the NTT and its inverse, NTT^{-1} , it is possible to efficiently compute the product of two polynomials in R_q , given that $\text{NTT}^{-1}(\hat{f} \cdot \hat{g}) = \text{NTT}^{-1}(\hat{h}) = h = f \cdot g$, calculated by fixing the following 128 products of polynomials $\hat{h}_{2i} + \hat{h}_{2i+1}x = (\hat{f}_{2i} + \hat{f}_{2i+1}x)(\hat{g}_{2i} + \hat{g}_{2i+1}x) \bmod (x^2 - \zeta^{2br(i)+1})$. The implementation of the NTT is shown in Figure 1b, where the roots of unity are previously calculated and stored in the matrix *zetas*. It can be appreciated that in the mathematical definition, as well as in the implementation, the process is iterative.

In Figure 1b, *len* represents the distance to which the operations are performed, this is why we define $k = 7 - \log_2(\text{len})$. Given that $\text{len} = 2^7 - k$, the further in the process the smaller is the operating distance. Variable *start* represents over which index of the vector *len* steps are made. As the definition is *len* plus the last value, $2 \cdot \text{len}$ steps are advanced. Finally, *j* represents the index of the vector over which each individual operation is executed, always between *j* and *j + len*. Moreover, *fmul* is an efficient implementation of modular multiplication. These expressions show that, mathematically, the transform is calculated independently on the parity of the index, whereas in the code *len* has values between 2^7 y 2^1 , meaning 7 iterations are performed. The *start* takes values which are multiples of *len* from 0 to 256, meaning the nested loop is executed 2^k times for each value of *len*, that is, $\sum_{i=1}^7 \frac{128}{2^i} = 128 \frac{127}{128}$ sums 128 roots of unity with the first *zeta* value. The last loop performs the multiplication of *zeta* and the corresponding value $r[j + \text{len}]$, in the interval $[\text{start} + \text{len}, 2 \cdot \text{len}]$ with $\text{len} - \text{start}$ iterations. Lastly, the transform adds each value to its symmetrical over *len* and subtracts it to the indexed value in the previous step. Figure 2 shows how the loop is executed in the implementation. It can be appreciated how each

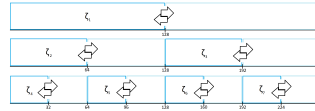


FIGURE 2. Illustration of NTT loop execution

iteration of *k* is represented with a row and each value of *start* with a colour. Variable *j* would be the one iterating over each colored block, indexing one by one $j = j + 1$. After a coloured block, *start* is increased $\text{start} = j + \text{len}$ until $\text{start} = \text{start} + 2 \cdot \text{len}$ that will start the next row. The arrows point which blocks are swapped, for each index *i* with its representative in the other block (starting from 0 in each block). Next step would be proposing a mathematical function that execute the process of the implementation in order to compare it to the original NTT. Representing each index of the vector by *i* and each iteration of the loop by *k*, knowing that $\text{len} = 2^7 - k$, we define the auxiliary recursive

function $\varphi_{i,k}$ as follows.

$$\begin{aligned} \varphi_{i,0} &= f_i + \zeta f_{i+128}, \quad 0 \leq i < 128, & \varphi_{i,0} &= f_{i-128} - \zeta f_i, \quad 128 \leq i < 256. \\ \varphi_{i,k} &= \varphi_{i,k-1} + \zeta^{2^k + \frac{i}{2^{8-k}}} \varphi_{i+2^{7-k},k-1}, & \varphi_{i,k} &= \varphi_{i-2^{7-k},k-1} + \zeta^{2^k + \frac{i}{2^{8-k}}} \varphi_{i,k-1} \end{aligned}$$

Finally, the starting call would be $\hat{f}_i = \varphi_{i,6}$. This way the base cases would represent the first iteration of the loop, when $len = 128$, and the following iterations, $0 < k < 7$, are determined by their parity in each iteration of $start$, or $start + len$. That is $i/2^{7-k} \bmod 2$ represents the division of the vector in intervals of length len and the mod 2 indicates whether its the left or right side. Each of the 128 *zeta* values is represented given that k and i can be at most 6 and 255 respectively. The greatest power of ζ would be $2^6 + 255/4 = 127$, covering all values from 1 to 127 (128 in total). Ultimately, the definition in the code greatly differs from the original one, mainly because the NTT is performed in the implementation over the coefficients of the polynomial. This could be one of the main reasons why side-channel attacks usually target the NTT in Kyber.

2. CONCLUSIONS

The differences shown between the mathematical definition, presented in the reference document of Kyber, and the official implementation, made by the original authors, are non negligible. These could lead to vulnerabilities that allow side-channel attacks that exploit them. In this first approach was not feasible to extract all possible vulnerabilities and soft spots with their possible repercussions. This is a complex topic and exhaustive analysis is needed to detect these discrepancies in the implementation. In our case, we highlighted the differences we spotted in our first analysis, emphasizing on the fragments of code that look more vulnerable, given that the mathematical operations specified in Kyber are far from simple. As a future line of investigation, we purpose two approaches: 1) analyzing and comparing the reference implementation of Kyber with the one present in other cryptolibraries, such as Open Quantum Safe (libOQS), and 2) developing an implementation of Kyber in interpreted languages, such as Sage or Maple, that permit to carry on some operations of Kyber in order to solve the discrepancies we spotted. This could even lead to deprecating the *poly_compress* and NTT operations by efficient implementations of polynomial multiplication. Note that it would be necessary to evaluate in terms of efficiency and security these propositions.

REFERENCES

- [1] E. Fujisaki and T. Okamoto, *Secure integration of asymmetric and symmetric encryption schemes*, Proc. Annual International Cryptology Conference, Advances in Cryptology - CRYPTO'99, Lecture Notes Comput. Sci., vol. 1666, 1999, https://doi.org/10.1007/3-540-48405-1_34, pp. 537–554.
- [2] Peter Schwabe, Roberto Avanzi, Joppe Bos, Leo Ducas, Eike Kiltz, Tancrede Lepoint, Vadim Lyubashevsky, John M. Schanck, Gregor Seiler, and Damien Stehle, *CRYSTALS-KYBER*, Online publication, 2020, <https://pq-crystals.org/kyber/index.shtml>.

Universidad Complutense de Madrid
Email address: diegroja@ucm.es

Instituto de Tecnologías Físicas y de la Información, CSIC
Email address: luis.h.encinas@csic.es

**PUNTOS DE INFLEXIÓN DE SUPERFICIES ALGEBRAICAS, UN
ENFOQUE MODERNO DEL TRABAJO DE GEORGE SALMON. /
INFLECTION POINTS OF ALGEBRAIC SURFACES, A MODERN
APPROACH TO THE WORK OF GEORGE SALMON.**

JORGE RODRÍGUEZ PÉREZ

ABSTRACT. Given an algebraic surface in complex three-dimensional projective space and a line passing through a point on this variety, the order of contact of the line with the surface can be defined as detailed in the article [2]. We call inflection points the points on the surface for which there exists a line with an order of contact greater than 3. In his book “A treatise on the analytic geometry of three dimensions” [3], George Salmon states that for an algebraic surface of degree d greater than or equal to 3, there exists a homogeneous polynomial that determines its inflection points. Furthermore, he provides an algorithm to calculate it which is due to Clebsch [1].

However, Salmon’s construction of this polynomial uses outdated notation, and the fields of algebraic geometry and resultant theory on which it relies have advanced significantly since his time. Although the general idea of the algorithm is mentioned in several articles, its computation has not yet been adapted to a modern mathematical language. The objective of this work is to adapt Salmon’s work to a modern notation, emphasizing which assumptions are necessary to apply the results that Salmon uses.

I started this work with Carlos D’Andrea in the first edition of Barcelona Introduction to Mathematical Research, summer 2022, and I am finishing it with Philippe Gimenez as my advisor as the final project of my mathematics studies at the University of Valladolid.

REFERENCES

- [1] Clebsch, A. (1861). Zur Theorie der algebraischen Flächen. *Journal für die reine und angewandte Mathematik (Crelles Journal)*, 1861(58), 93–108. <https://doi.org/10.1515/crll.1861.58.93>
- [2] Busé, L., D’Andrea, C., Sombra, M., and Weimann, M. (2020). The geometry of the flex locus of a hypersurface. *Pacific Journal of Mathematics*, 304(2), 419–437. <https://doi.org/10.2140/pjm.2020.304.419>
- [3] Salmon, G. (1915). *A treatise on the analytic geometry of three dimensions* (R. A. P. Rogers, Ed., Vol. 2). Retrieved from <https://archive.org/details/cu31924001521065>

University of Valladolid

Email address: jorge.rodriguez@uva.es