

Proceedings of  
**A**pplications of **C**omputer **A**lgebra  
**ACA 2013. Málaga**

July 2nd-6th, 2013  
Hotel Málaga Palacio.  
Málaga, Spain



Editors:

**José Luis Galán García**  
**Gabriel Aguilera Venegas**  
**Pedro Rodríguez Cielos**

ISBN-10: **84-616-4565-0**  
ISBN-13: **978-84-616-4565-7**  
Reg. Number: **201336327**

Proceedings of Applications of Computer Algebra 2013.

Editors:

José Luis Galán García  
Gabriel Aguilera Venegas  
Pedro Rodríguez Cielos

ISBN-10: **84-616-4565-0**

ISBN-13: **978-84-616-4565-7**

Reg. Number: **201336327**

Contact: [aca2013@ctima.uma.es](mailto:aca2013@ctima.uma.es)

Web: <http://aca2013.uma.es/>

Printed in Spain  
July 2013

Composition developed by editors using L<sup>A</sup>T<sub>E</sub>X.

# Contents

<b>Prologue</b>	<b>9</b>
Prologue . . . . .	11
<b>Chairs &amp; Committees</b>	<b>13</b>
General Chairs . . . . .	15
Program Chairs . . . . .	15
Advisory Committees . . . . .	15
Local Chairs . . . . .	15
Scientific Committee . . . . .	15
<b>Plenary Lectures</b>	<b>17</b>
<b>10 years of sequence autocorrelation</b>	
Ilias Kotsireas . . . . .	19
<b>Some ideas about the research in computational mathematics: a perspective from the middle of the life and the academic life</b>	
Eugenio Roanes-Lozano . . . . .	20
<b>Session 0: General Session on Computer Algebra</b>	<b>25</b>
<b>A New Criterion for the Existence of Real Zeros of Polynomial Systems</b>	
Jin-San Cheng . . . . .	27
<b>Planar arrangements and singular algebraic surfaces</b>	
Juan Escudero . . . . .	28
<b>Computations of Gröbner-Shirshov Basis and Reduced Words for Affine Weyl Group <math>\tilde{A}_n</math> using Mathematica</b>	
Erol Yılmaz, Cenap Özel, Uğur Ustaoglu . . . . .	33
<b>Session 1: Computer Algebra in Education</b>	<b>35</b>
<b>CAS: A Tool for Improving Students' Autonomous Work</b>	
Alfonsa García, Francisco García, Ángel Martín del Rey, Gerardo Rodríguez, Agustín de la Villa . . . . .	37
<b>Assessing Mathematical Content in a Technology Environment Discussion Panel</b>	
Ángel Homero Flores . . . . .	38
<b>Global application of CAS tools for teaching in Computer Engineering degrees</b>	
Santiago Cárdenas, Inmaculada Fortes, Inmaculada Pérez de Guzmán, Sixto Sánchez, Agustín Valverde . . . . .	41

<b>In praise of rectangular systems</b>	
David Jeffrey . . . . .	42
<b>Polynomial Systems Solving with Nspire CAS (Part I, Part II)</b>	
Michel Beaudin, Gilles Picard, Geneviève Savard . . . . .	43
<b>Some maths problems for the average citizen</b>	
Eugenio Roanes-Lozano, Justo Cabezas-Corchero . . . . .	44
<b>Investigating Magic Squares in a Linear Algebra Course</b>	
Karsten Schmidt . . . . .	47
<b>Computer Algebra - the engine of transition to activity-based approach in mathematics education</b>	
Elena Varbanova, Elena Shoikova . . . . .	48
<b>Using Computer Algebra in Mathematics for Engineers</b>	
Thomas Westermann . . . . .	49
<b>Omega: A Free Computer Algebra System Explorer for Online Education</b>	
Michael Xue . . . . .	50

**Session 2: Computer Algebra for Dynamical Systems and Celestial Mechanics** **55**

<b>On necessary conditions of integrability of degenerated planar ODE systems in the parameter space</b>	
Alexander Bruno, Victor Edneral . . . . .	57
<b>On using computer algebra systems for analysis of rigid body dynamics</b>	
Larisa Burlakova, Valentin Irtegov . . . . .	58
<b>Orbital Reversibility of Dynamical Systems</b>	
Antonio Algaba, Isabel Checa, Cristóbal García, Estanislao Gamero . . . . .	63
<b>The Study of Isochronicity and Critical Period Bifurcations on Center Manifolds of 3-dim Polynomial Systems Using Computer Algebra</b>	
Matej Mencinger, Brigita Fercec . . . . .	68
<b>Formal Integral and Caustics in Henon-Heiles model</b>	
Tatiana Myllari, Aleksandr Myllari . . . . .	73
<b>Tree structures in Poisson series processors</b>	
Juan F. Navarro . . . . .	74
<b>Normal Forms of Singular Plane Quartics</b>	
Tadashi Takahashi . . . . .	79

**Session 3: Algebraic and Algorithmic Aspects of Differential and Integral Operators Session** **81**

<b>Seeking recursion operators - an universal hierarchy example in dimension <math>(2 + 1)</math></b>	
Hynek Baran . . . . .	83
<b>The algebra of polynomial integro-differential operators and its group of automorphisms</b>	
V. V. Bavula . . . . .	84
<b>Darboux theory of integrability in the sparse case</b>	
Guillaume Chèze . . . . .	85
<b>Isomorphisms and Serre's reduction of multidimensional linear systems</b>	
Thomas Cluzeau, Alban Quadrat . . . . .	86
<b>Qualitative Study of Polynomial Differential Systems</b>	
Dahira Dali, Abdo Turki . . . . .	87
<b>Periodic and Mean-Periodic Solutions of LODEs with Constant Coefficients</b>	
Ivan Dimovski, Margarita Spiridonova . . . . .	92
<b>Looking for invariant algebraic curves</b>	
Antoni Ferragut, Armengol Gasull . . . . .	93
<b>Moving Frames and Noether's Conservation Laws - the General Case</b>	
Tânia M. N. Gonçalves, Elizabeth L. Mansfield . . . . .	95

<b>Interpolation with integral and Stieltjes conditions</b>	
Anja Korporal, Georg Regensburger . . . . .	96
<b>On Completely Integrable Pfaffian Systems with Normal Crossings</b>	
Suzy Maddah . . . . .	97
<b>Linear Boundary Problems for Partial Differential Equations: Algebraic Setup and First Steps for Constant Coefficients</b>	
Nalina Phisanbut, Markus Rosenkranz . . . . .	99
<b>On the arithmetic of d'Alembertian functions</b>	
Clemens Raab . . . . .	100
<b>Applying Thomas decomposition and algebraic analysis to certain nonlinear PDE systems</b>	
Daniel Robertz . . . . .	101
<b>Sparse differential resultant formulas: between the linear and the nonlinear case</b>	
Sonia L. Rueda . . . . .	102
<b>Session 4: Computer Algebra in Coding Theory and Cryptography</b>	<b>107</b>
<b>A characterization of cyclic codes whose minimum distance equals their maximum BCH bound</b>	
J. J. Bernal, D. H. Bueno, J. J. Simon . . . . .	109
<b>Gröbner Bases and Linear Codes over Prime Fields</b>	
Natalia Dück, Karl-Heinz Zimmermann . . . . .	114
<b>A Class of Binary Sequences with Large Linear Complexity</b>	
Amparo Fúster Sabater . . . . .	118
<b>Further Improvements on the Feng-Rao Bound for Dual Codes</b>	
Olav Geil, Stefano Martin . . . . .	120
<b>Some Optimal Codes as Tanner Codes with BCH Component Codes</b>	
Tom Høholdt, Fernando Piñero, Peng Zeng . . . . .	122
<b>A secret sharing scheme using Gröbner basis</b>	
Hiroshi Kai, Masaki Yamada . . . . .	127
<b>Error-correcting pairs and arrays from algebraic geometry codes</b>	
Irene Márquez-Corbella, Ruud Pellikaan . . . . .	129
<b>Additive multivariable codes over <math>F_4</math></b>	
E. Martínez-Moro, A. P. Nicolás, I. F. Rua . . . . .	133
<b>On Generalized Lee Weigth Codes over Dihedral Groups</b>	
E. Martínez-Moro, A. P. Nicolás, E. Suárez-Canedo . . . . .	134
<b>Decoding of codes for applications to steganography</b>	
Carlos Munuera, Wilson Olaya León . . . . .	135
<b>On LDPC codes corresponding to new families of regular expanding graphs of large girth</b>	
Monika Polak, Vasyl Ustymenko . . . . .	137
<b>Representation, constructions and minimum distance computation of binary non-linear codes</b>	
J. Pujol, M. Villanueva, F. Zeng . . . . .	142
<b>On regular forests given in terms of algebraic geometry, new families of expanding graphs with large girth and new multivariate cryptographical algorithms</b>	
Urszula Romańczuk, Vasyl Ustymenko . . . . .	144
<b>Some remarks for codes and lattices over imaginary quadratic fields</b>	
T. Shaska, C. Shor . . . . .	148
<b>An Efficient Algorithm for Computing Branch Groebner Systems and Its Applications in Algebraic Cryptanalysis</b>	
Yao Sun, Zhenyu Huang, Dongdai Lin, Ding kang Wang . . . . .	153
<b>On some algebraic aspects of data security in cloud computing</b>	
Vasyl Ustymenko, Aneta Wroblewska . . . . .	155

<b>Session 5: Nonstandard Applications of Computer Algebra</b>	<b>161</b>
<b>Similarity Detection for Rational Curves</b>	
Juan G. Alcázar, Carlos Hermoso, Georg Muntingh . . . . .	163
<b>Envelope computation in dynamic geometry systems</b>	
Francisco Botana, Tomás Recio . . . . .	164
<b>Obtaining combinatorial structures associated with low-dimensional Leibniz algebras</b>	
Manuel Ceballos, Juan Núñez, Ángel F. Tenorio . . . . .	168
<b>Designing Hamiltonian Cycles</b>	
Francisco de Arriba, Eusebio Corbacho, Ricardo Vidal . . . . .	173
<b>Designing rotating schedules by using Gröbner bases</b>	
Raúl Falcón, David Canca, Eva Barrena . . . . .	178
<b>Simulating Car Traffic with Smart Signals using a CAS</b>	
José Luis Galán, Gabriel Aguilera, José Carlos Campos, Pedro Rodríguez . . . . .	183
<b>Padovan-like sequences and Bell polynomials</b>	
Nikita Gogin, Aleksandr Mylläri . . . . .	184
<b>Modeling reliability in propositions using computer algebra techniques</b>	
Antonio Hernando . . . . .	187
<b>Flexibility of Structures via Computer Algebra</b>	
Robert H. Lewis, Evangelos Coutsias . . . . .	192
<b>A hybrid expert system for classic car recognition and originality evaluation</b>	
Eugenio Roanes-Lozano, Jesús Bonilla . . . . .	193
<b>Populational-based anamorphosis maps for railway radial networks</b>	
Eugenio Roanes-Lozano, Alberto García-Álvarez, José Luis Galán-García, Luis Mesa . . . . .	194
<b>An algebraic approach to geometric proof using a Computer Algebra System</b>	
Michael Xue . . . . .	197
<b>Session 6: Arithmetic of Algebraic Curves</b>	<b>201</b>
<b>Hyperbolic uniformizations through computations on ternary quadratic forms</b>	
M. Alsina . . . . .	203
<b>Symplectic representations for finite group actions on Riemann surfaces</b>	
Antonio Behn, Anita Rojas, Rubí Rodríguez . . . . .	207
<b>On superelliptic curves and their Jacobians</b>	
T. Shaska, L. Beshaj . . . . .	208
<b>On the automorphisms groups of Hassett moduli spaces</b>	
Alex Massarenti . . . . .	212
<b>From relations in the moduli spaces of curves, to recursions in Gromov-Witten theory</b>	
N. Pagani . . . . .	218
<b>On the Approximate Parametrization Problem of Algebraic Curves</b>	
Sonia L. Rueda, J. Rafael Sendra, Juana Sendra . . . . .	219
<b>Radical parametrization of algebraic curves and surfaces</b>	
D. Sevilla, J. Rafael Sendra . . . . .	224
<b>Weierstrass points and dihedral invariants of superelliptic curves</b>	
C. Shor, T. Shaska . . . . .	229
<b>Session 7: Applications and Libraries development in DERIVE and TI-NSPIRE</b>	<b>235</b>
<b>FOPDE.mth: Solving First-Order Partial Differential Equations with DERIVE 6 step by step</b>	
Gabriel Aguilera, José Luis Galán, María Ángeles Galán, Yolanda Padilla, Pedro Rodríguez, Ricardo Rodríguez . . . . .	237

<b>Integration of Piecewise Continuous Functions (Part I, Part II)</b>	
Michel Beaudin, Frédéric Henri, Geneviève Savard . . . . .	238
<b>A Toolbox with DERIVE: Calculus on Several Variables</b>	
Alfonsa García, Francisco García, Ángel Martín del Rey, Gerardo Rodríguez, Agustín de la Villa . . . . .	239
<b>DERIVE and Linear Algebra</b>	
Alfonsa García, Francisco García, Ángel Martín del Rey, Gerardo Rodríguez, Agustín de la Villa . . . . .	240
<b>A Dynamic Unity of Tradition and Technology in Undergraduate Mathematics - a Bulgarian Experience</b>	
Elena A. Varbanoba . . . . .	241
<b>Session 8: Computer Algebra in Algebraic Statistics</b>	<b>243</b>
<b>Computing real log canonical thresholds in algebraic statistics</b>	
Hamid Ahmadinezhad, Josef Schicho, Caroline Uhler . . . . .	245
<b>Error evaluation for algebraic interpolatory cubature formulae</b>	
Claudia Fassino, Eva Riccomagno . . . . .	250
<b>A Gröbner Bases Method for Complementary Sequences</b>	
Christos Koukouvinos, Dimitris E. Simos, Zafeirakis Zafeirakopoulos . . . . .	255
<b>Goodness-of-fit testing in Ising Models</b>	
Abraham Martín del Campo, Caroline Uhler . . . . .	260
<b>Monomial ideal methods for hierarchical statistical models</b>	
Hugo Maruri-Aguilar, Eduardo Sáenz-de-Cabezón, Henry P. Wynn . . . . .	261
<b>Algebraic geometry in causal inference</b>	
Caroline Uhler . . . . .	262
<b>Connectivity on two-way tables under certain models</b>	
Ruriko Yoshida . . . . .	263
<b>Session 9: Computer algebra, quantum computing and quantum information processing</b>	<b>269</b>
<b>On the inequalities defining the entanglement space of 2-qubits</b>	
V. P. Gerdt, A. M. Khvedelidze, Yu. G. Pali . . . . .	271
<b>Mathematica Package Quantum Circuit for Simulation of Quantum Computation</b>	
V. P. Gerdt, A. N. Prokopenya . . . . .	274
<b>Simulating quantum computers with Mathematica: QDENSITY et al.</b>	
Bruno Julia-Diaz, Frank Tabakin . . . . .	275
<b>Functional framework for representing and transforming quantum channels</b>	
Jarosław Adam Mischak . . . . .	276
<b>Ultimate limits to squeezing of quantum fluctuations</b>	
Arkadiusz Orłowski . . . . .	281
<b>Geometry and Dynamics of Algorithms on the Quantum Information Space</b>	
Yoshio Uwano . . . . .	282
<b>Session 10: Computer algebra in algebraic topology and its applications</b>	<b>287</b>
<b>On Higher Dimensional Cocyclic Hadamard Matrices</b>	
Victor Álvarez Solano, José Andrés Armario, María Dolores Frau, Pedro Real . . . . .	289
<b><math>A_\infty</math>- persistence</b>	
Kiko Belchí, Aniceto Murillo Mas . . . . .	290
<b>Discrete Morse Theory and Computational Homology</b>	
Pawel Dlotko . . . . .	291

<b>Some Advanced in G-invariant topology and homology</b>	
Patrizio Frosini . . . . .	292
<b>Boundary and Acyclicity Operators of Primal and Dual Elementary Cell Complexes</b>	
Ana María Pacheco, Pedro Real . . . . .	293
<b>A chain contraction approach to the computation of cubical homology and cohomology</b>	
Paweł Pilarczyk, Pedro Real . . . . .	294
<b>Computational Homological Algebra for Advanced Topological Analysis of 4D Digital Images</b>	
Pedro Real . . . . .	295
<b>Spectral Sequences for computing persistent homology of digital images</b>	
Ana Romero, Gadea Mata, Julio Rubio, Jonathan Heras, Francis Sergeraert . . . . .	297
<b>Session 11: Symbolic and Numerical Methods: Practical Applications</b>	<b>299</b>
<b>A numerical and an exact approaches for classifying the items of a questionnaire into different competences</b>	
José Luis Galán, Salvador Merino, Javier Martínez, Miguel de Aguilera . . . . .	301
<b>Optimization and design of bicycles lines</b>	
Roberto José Liñan, Salvador Merino, Javier Martínez . . . . .	303
<b>Resolution of solar cells equivalent electrical model by reverse decomposition</b>	
Salvador Merino, Francisco J. Sánchez, Pedro Rodríguez, Carlos Sánchez . . . . .	308
<b>Using CUDA for better harnessing of symbolic and numerical methods</b>	
S. Ortega Acosta, J. M. González Vida, M. L. Muñoz Ruiz, C. Sánchez Linares, T. Morales de Luna . . . . .	309
<b>Numerical algorithm solves for a new positioning system inside buildings</b>	
Ana Belén Pabón, Salvador Merino, Pedro Rodríguez . . . . .	310
<b>Kinematical analysis of mechanisms with computer algebra</b>	
Samuli Piipponen, Teijo Arponen, Jukka Tuomela . . . . .	311
<b>CAS software for teaching numerical methods in engineering. Practical applications</b>	
C. Sánchez Linares, J. M. González Vida, T. Morales de Luna, M. L. Muñoz Ruiz, S. Ortega Acosta . . . . .	312
<b>Statistical Quality Control in the Construction Industry</b>	
José Antonio Vera, Salvador Merino, José Luis Galán . . . . .	313
<b>List of Participants</b>	<b>319</b>
List of Participants . . . . .	321
<b>Authors Index</b>	<b>325</b>
<b>Appendix</b>	<b>329</b>
<b>Spectral Sequences for computing persistent homology of digital images</b>	
Ana Romero, Gadea Mata, Julio Rubio, Jonathan Heras, Francis Sergeraert . . . . .	331



---

---

# Prologue

---

---



# Prologue

Dear colleagues,

It is our pleasure to welcome you to Málaga for **ACA 2013** (Applications of Computer Algebra).

The ACA conference series is devoted to promoting all manner of computer algebra applications, and encouraging the interaction of developers of computer algebra systems and packages with researchers and users (including scientists, engineers, educators, etc.). Topics include, but are not limited to, computer algebra in the sciences, engineering, medicine, pure and applied mathematics, education and computer science.

ACA Conferences are run in different Special Sessions. In ACA 2013, the following 12 Special Sessions have been accepted:

- Session 0: General Session on Computer Algebra  
Organizers: José Luis Galán García, Gilles Picard.
- Session 1: Computer Algebra in Education  
Organizers: Michel Beaudin, Michael Wester, José Luis Galán García, Alkis Akritas, Bill Pletsch, Elena Varbanova.
- Session 2: Computer Algebra for Dynamical Systems and Celestial Mechanics  
Organizers: Victor Edneral, Aleksandr Myllari, Valery Romanovski, Nikolay Vassiliev.
- Session 3: Algebraic and Algorithmic Aspects of Differential and Integral Operators Session  
Organizers: Moulay Barkatou, Thomas Cluzeau, Georg Regensburger, Markus Rosenkranz.
- Session 4: Computer Algebra in Coding Theory and Cryptography  
Organizers: Ilias Kotsireas, Edgar Martínez-Moro.
- Session 5: Nonstandard Applications of Computer Algebra  
Organizers: Francisco Botana, Antonio Hernando, Eugenio Roanes-Lozano, Michael Wester.
- Session 6: Arithmetic of Algebraic Curves  
Organizers: Jean-Marc Couveignes, Nicola Pagani, Tony Shaska.
- Session 7: Applications and Libraries development in DERIVE and TI-NSPIRE  
Organizers: José Luis Galán García, Pedro Rodríguez Cielos, Gabriel Aguilera Venegas, Josef Böhm.
- Session 8: Computer Algebra in Algebraic Statistics  
Organizers: Hugo Maruri-Aguilar, Eduardo Sáenz-de-Cabezón, Henry P. Wynn.
- Session 9: Computer algebra, quantum computing and quantum information processing  
Organizers: Vladimir Gerdt, Alexander Prokopenya, Yoshia Uwano.
- Session 10: Computer algebra in algebraic topology and its applications  
Organizers: Aniceto Murillo, Pedro Real, Eduardo Sáenz-de-Cabezón.
- Session 11: Symbolic and Numerical Methods: Practical Applications  
Organizers: José Manuel González Vida, Tomás Morales de Luna, María Luz Muñoz Ruiz.

From the very beginning, ACA Conferences have been a very important meeting point for professionals in the use of Computer Algebra in different fields. In this occasion, ACA 2013 has joined 109 delegates from 25 different countries and a total of 124 participants.

105 contributions have been finally accepted by session organizers. This proceedings book contents the extended abstracts of these 105 contributions together with two more extended abstracts from the Plenary Lectures.

The editors deeply thank to:

- Gilles Picard, Program Chair, not only for all his work within organization matters, but also for his continuous support.
- Eugenio Roanes-Lozano, Stanly Steinberg and Michael Wester, the Advisory Committee, for all their work, help, suggestions and support regarding organization.
- ACA-WG Members for their work in the review process when dealing with session proposals.
- Session organizers, for their work in the review process of the talk proposals and for the organizing their sessions.
- Eugenio Roanes-Lozano and Ilias Kotsireas for accepting the offer of being keynote speakers and providing 2 wonderful and very interesting keynote lectures.
- Salvador Merino Córdoba, Javier Martínez del Castillo, M<sup>a</sup> Ángeles Galán García, Yolanda Padilla Domínguez, M<sup>a</sup> Luz Muñoz Ruiz and José Manuel González Vida, the Local Chairs. Without their work, this meeting would have been significantly different. We also want to thank in this point our students from the local organization, for their invaluable help.
- And last but not least, all the participants (both delegates and accompanying persons) for their interest and contribution to make this meeting to be a very important event.

Málaga, July 2013

The editors:  
José Luis Galán García  
Gabriel Aguilera Venegas  
Pedro Rodríguez Cielos

---

---

## Chairs & Committees

---

---



# Chairs and Committees

## General Chairs

José Luis Galán García, Spain  
Pedro Rodríguez Cielos, Spain  
Gabriel Aguilera Venegas, Spain

## Program Chairs

José Luis Galán García, Spain  
Gilles Picard, Canada

## Advisory Committee

Eugenio Roanes-Lozano, Spain  
Stanly Steinberg, USA  
Michael Wester USA

## Local Chairs

Salvador Merino Córdoba, Spain  
Javier Martínez del Castillo, Spain  
M<sup>a</sup> Ángeles Galán García, Spain  
Yolanda Padilla Domínguez, Spain  
M<sup>a</sup> Luz Muñoz Ruiz, Spain  
José Manuel González Vida, Spain

## Scientific Committee

ACA conferences are under the supervision of the Applications of Computer Algebra Working Group (ACA WG):

Alkiviadis Akritas, Michel Beaudin, Bruno Buchberger, Jacques Calmet, Victor Edneral, José Luis Galán García, Victor Ganzha, Vladimir Gerdt, Mark Giesbrecht, Hoon Hong, David Jeffrey, Hiroshi Kai, Erich Kaltofen, Ilias Kotsireas, Bernhard Kutzler, Robert H. Lewis, Richard Liska, Winfried Neun, Matu-Tarow Noda, Gilles Picard, Kathleen Pineau, Bill Pletsch, Eugenio Roanes-Lozano (ACA WG Chair), Tateaki Sasaki, Yosuke Sato, Tony Shaska, Margarita Spiridonova, Stanly Steinberg (founder of the ACA conference series), Agnes Szanto, Quoc-Nam Tran, Nikolay Vasiliev, Stephen Watt, Michael Wester (co-founder of the ACA conference series), Wolfgang Windsteiger, Franz Winkler





---

---

# Plenary Lectures

---

---

**Organizers:**

**José Luis Galán García  
Gilles Picard**



# 10 years of sequence autocorrelation

Ilias S. Kotsireas  
Wilfrid Laurier University (Canada)

ikotsire@wlu.ca

## Abstract

The autocorrelation functions (periodic and aperiodic) associated to finite sequences have been the object of intense study in Discrete Mathematics and Combinatorics. Finite sequences whose autocorrelation functions sum to a constant are called complementary sequences. The search for complementary sequences is a very challenging problem from the theoretical and algorithmic point of view. In our work for the past 10 years we have developed with our collaborators various algorithmic techniques (and significantly improved existing methods) to search efficiently for complementary sequences. An important aspect of complementary sequences is the fact that they can be used to construct D-optimal, Hadamard and weighing matrices, among many other combinatorial objects. I plan to summarize our achievements with a special focus on recent successes [2], [3], [6], [7] using cyclotomy-based methods and metaheuristics methods. I also plan to point out important connections of specific kinds of complementary sequences with Coding Theory [4]. Complementary sequences problems can be formulated as systems of polynomial equations (with typically a few hundred variables) that exhibit symmetries. Therefore the Symbolic Computation methods of [1] come into play. High-performance computing (also known as supercomputing) is another important ingredient of algorithms pertaining to the search for complementary sequences. The interested reader can also consult my recent chapter [5] for more information, detailed examples and extensive bibliography on these topics.

## Keywords

autocorrelation, complementary sequences, Hadamard matrices, weighing matrices

## References

- [1] Robert M. Corless, Karin Gatermann, Ilias S. Kotsireas, Using symmetries in the eigenvalue method for polynomial systems. *J. Symbolic Comput.* 44 (2009), no. 11, pp. 1536–1550.
- [2] Dragomir Z. Djokovic, Ilias S. Kotsireas, New results on D-optimal matrices, *Journal of Combinatorial Designs* Volume 20, Issue 6, June 2012, pp. 278-289.
- [3] Dragomir Z. Djokovic, Oleg Golubitsky, Ilias S. Kotsireas, Some new orders of Hadamard and skew-Hadamard matrices, *Journal of Combinatorial Designs*, ACCEPTED
- [4] Ilias S. Kotsireas, *Structured Hadamard Conjecture*, in: Number Theory and Related Fields, In Memory of Alf van der Poorten, Springer Proceedings in Mathematics & Statistics, Vol. 43, Jonathan M. Borwein, Igor Shparlinski, Wadim Zudilin, (Eds.) 2013 pp. 215–227.
- [5] Ilias S. Kotsireas, Algorithms and Meta-heuristics for Combinatorial Matrices, chapter in: *Handbook of Combinatorial Optimization*, 2nd Edition, edited by: Panos M. Pardalos, Ding-Zhu Du, and Ron Graham TO APPEAR
- [6] Ilias S. Kotsireas, Panos M. Pardalos, D-optimal Matrices via Quadratic Integer Optimization, *Journal of Heuristics* TO APPEAR
- [7] Ilias S. Kotsireas, Konstantinos E. Parsopoulos, Grigoris Piperagkas, Michael N. Vrahatis, Ant-Based Approaches for Solving Autocorrelation Problems, ANTS 2012, September 12-14, 2012, Brussels, Belgium. Lecture Notes in Computer Science (LNCS), Vol. 7461, pp. 220–227, Springer (2012).

# Some ideas about the research in computational mathematics: a perspective from the middle of the life and the academic life (Plenary Talk)

Eugenio Roanes-Lozano  
Instituto de Matemática Interdisciplinar (IMI),  
Departamento de Álgebra, Facultad de Educación,  
Universidad Complutense de Madrid, E-28040 Madrid (Spain)

`eroanes@mat.ucm.es`

## Abstract

The author gives an overview of his education and his experience in applied computational mathematics research.

## Keywords

Effective computations, Railway interlocking systems, Gröbner bases, Simulation, Motivation.

## 1 Extended Abstract

### 1.1 ACA conference series

I have attended all ACA conferences except ACA'2005 and ACA'2010 and I organized ACA'1999 at El Escorial (Spain).

In 2003 I was invited by Prof. Hoon Hong to be the banquet speaker at ACA'2003 (Raleigh, NC).

Now, ten years older, Prof. José Luis Galán has invited me to address you again as plenary speaker. I would like to thank Prof. Galán and the different committees of ACA'2013 for this opportunity.

### 1.2 My mathematical education and the outside world

I'm the son of a mathematician, Eugenio Roanes-Macías (an algebrist whose Ph.D. advisor was Prof. Pedro Abellanas, a disciple of Prof. Wolfgang Krull). He dedicated a good part of his time to my mathematical education since I was a young boy.

I studied mathematics at the Universidad Complutense de Madrid. I never used a computer while at university (1979-1984). Just to mention some of my teachers, I enjoyed discovering real analysis with Prof. Baldomero Rubio, linear geometry with Prof. Javier Etayo and differential equations and control theory with Prof. Miguel de Guzmán. And a crossroad in my academic life was discovering axiomatic-systems with Prof. María Paz Bujanda.

But I also discovered some deceptions regarding mathematic. The biggest one was to learn in a post-graduate course taught by Prof. Luis Laita (my other master), the existence of paradoxes and Gödel's incompleteness theorem. The beautiful mathematical building I was beginning to visit was not absolutely perfect...

The other one had happened earlier, when I studied algebraic geometry during my third year at university. The theory was perfectly developed, we studied very long and detailed proofs, but the examples presented to us were trivial (normally only lines, planes, conics and quadrics were used, and the applications of the results to the examples were many times obvious or trivial) and apparently with no application. I then thought about leaving my studies and switching to mechanical engineering.

### 1.3 The outside world... and crisis

So far I had defended mathematics from questions like:

*“Why are you going to study mathematics for? Become a physician, like your grandfather. That’s useful.”*

or attacks like:

*“Are mathematics useful? I don’t have a clue of any use in my everyday life...”*

I answered with ideas that I had heard to my father, like

*“Mathematics is behind everything: from technological items like a car, a building, a bridge,... to arts like music, painting,...”*

(ideas close to those shown in the beautiful Disney’s film “Donald in Mathematicland”, or:

*“You can study a theoretical subject like commutative algebra or theoretical physics just for the pleasure of discovering.”*

But I began to doubt... Were “those mathematics” my real passion?

### 1.4 Effective computations

I started my thesis in commutative algebra with my father as advisor not very enthusiastically. But all that changed after beginning to work with the computer algebra system *REDUCE* in 1987 and after attending a post-graduate course taught by Prof. Franz Winkler (whose advisor was Prof. Bruno Buchberger) about Gröbner bases. As a consequence, the last part of my Ph.D. thesis included effective computations, what was very exciting to me. Moreover, Prof. Tomás Recio introduced me to mechanical theorem proving in geometry in 1988.

The possibility of performing effective computations in Euclidean geometry, algebraic geometry and commutative algebra changed my attitude towards these disciplines: they became attractive to me again!!! I was so energetic that I prepared a second thesis in computer science (the Ph.D. advisors were my father and, curiously, Prof. Manuel Abellanas, son of Prof. Pedro Abellanas).

Afterwards, I begun working with Prof. Luis Laita in the applications of computer algebra to logic and artificial intelligence, a very long and fruitful cooperation.

### 1.5 Hobbies and research

Railways (together with cars) have been my passion since I was a child. Visiting the railway station just to watch trains has always been at pleasure for me. In 1981, I obtained the Spanish Philips<sup>1</sup> “Premio Holanda” (a young researcher award) for a theoretical proposal entitled “Block-system with mobile sections”, where some of the key ideas of the modern “European Train Control System” (ETCS) were sketched.

Of all my papers, my favourite one is probably the one adapting Gröbner bases to decision making in a railway interlocking system<sup>2</sup>. In fact this has been my most active line of research: we have developed matrix [1], Gröbner bases [2, 3], logic [4] and logic-algebraic [5] models. These models, although implemented, have never been applied to real life because it is very difficult (and expensive) to have safety-critical applications approved.

**I’ll give in this talk an overview of these approaches to decision making in a railway interlocking, most of them presented at the “Applications of Computer Algebra (ACA)” conference series.**

Curiously, although not directly applied, these works have been the key to most of my present lines of research and its funding (from both the Government of Spain and also private funding). Regarding the latter, I specifically note:

- Passenger movement simulation within an airport (Spanish Airport Authority, 2003) [6] and railway traffic simulation [7].

---

<sup>1</sup>The big Dutch electronics company.

<sup>2</sup>Railway interlocking systems are apparatuses that prevent conflicting movements of trains through an arrangement of tracks. A railway interlocking system takes into consideration the position of the switches of the turnouts and does not allow trains to be given clear signals unless the routes to be used by the trains do not intersect.

- Routing and timing of trains in the complex Spanish railway network (Spanish Railways Foundation, 2010) [8].
- Costs and emissions of trains in the complex Spanish railway network (Spanish Railways Foundation, 2011) [9].

Many of the railways-related works have been developed in cooperation with Dr. Alberto García-Álvarez, Executive Director of Passengers for Renfe (Spanish Railways).

My computer algebra applied works were also the key to my involvement in the organization of the conferences “Applications of Computer Algebra (ACA)” and “Artificial Intelligence and Symbolic Computation (AISC)”, thanks to the kindness and dedication of Prof. Stanly Steinberg and Prof. Michael Wester in the first case and Prof. Jacques Calmet and Prof. John Campbell in the second case.

## 1.6 The usefulness of a research

One of the favourite examples of my father (originally a physicist) when asked about the utility of theoretical “useless” mathematics were geometries in dimension greater than 3 and the works of Gauss, Lobachevski and others about non-Euclidean geometries (all apparently useless academic exercises) and their ultimate application to relativity theory by Minkowski.

Obviously I’m not comparing my works with those of geniuses like Gauss, Lobachevski or Minkowski, but I’ve tried to emphasize in the previous section that such situations also arise in computational mathematics, not only in “pure mathematics” and that they can happen at “normal” levels.

## 1.7 Conclusions

Summarizing, as my advise to young researchers in computational mathematics:

- Working in what you love is, by default, fruitful.
- Using techniques from a certain field in a very different field is usually very innovative and fruitful.
- Never abandon a fruitful research line that you like for its apparent lack of direct application: it could have a future one.
- It is worthwhile making an effort to meet people in one’s field and talking to them (via conferences, visits, etc.). Actually organizing a meeting also allows one to meet a lot of people.

## Acknowledgments

I would like to thank Prof. Michael Wester for improving the English of this Extended Abstract.

## References

- [1] Roanes-Lozano, E., Laita, L.M.: An applicable topology-independent model for railway interlocking systems. *Math. Comput. Simul.* 45(1), 175–184 (1998).
- [2] Roanes-Lozano, E., Laita, L.M., Roanes-Macías, E.: An application of an AI methodology to railway interlocking systems using computer algebra. In: Pasqual del Pobil, A., Mira, J., Ali, M. (eds.) *Tasks and Methods in Applied Artificial Intelligence, Proceedings of IEA-98-AIE*, vol. II. Springer LNAI, vol. 1416, pp. 687–696. Berlin, Heidelberg (1998)
- [3] Roanes-Lozano, E., Roanes-Macías, E., Laita, L.M.: Railway interlocking systems and Gröbner bases. *Math. Comput. Simul.* 51(5), 473–481 (2000)
- [4] Roanes-Lozano, E., Hernando, A., Alonso, J.A., Laita, L.M.: A logic approach to decision taking in a railway interlocking system using maple. *Math. Comput. Simul.* 82(1), 15–28 (2011).

- [5] Hernando, A., Roanes-Lozano, E., Maestre-Martínez, R., Tejedor, J.: A logic-algebraic approach to decision taking in a railway interlocking system. *Annals Math. Artif. Intell.* 65(4), 317–328 (2012).
- [6] Roanes-Lozano, E., Laita, L.M., Roanes-Macías, E.: An accelerated-time simulation of departing passengers' flow in airport terminals. *Math. Comput. Simul.* 67(1–2), 163–172 (2004).
- [7] Hernando, A., Roanes-Lozano, E., García-Álvarez, A.: An accelerated-time microscopic simulation of a dedicated freight double-track railway line *Mathematical and Computer Modelling*, 51(9–10), 1160–1169 (2010).
- [8] Hernando, A., Roanes-Lozano, E., García-Álvarez, A., Mesa, L., González-Franco, I.: Optimal Route Finding and Rolling-Stock Selection for the Spanish Railways. *Comput. Sci. Eng.* 14(4), 82–89 (2012).
- [9] Roanes-Lozano, E., Hernando, A., García-Álvarez, A., Mesa, L., González-Franco, I.: Calculating the exploitation costs of trains in the Spanish railways. *Comput. Sci. Eng.* (2013, to appear).





---

---

# Session 0: General Session on Computer Algebra

---

---

Organizers:

José Luis Galán García  
Gilles Picard



# A New Criterion for the Existence of Real Zeros of Polynomial Systems

Jin-San Cheng

KLMM, Institute of Systems Science, AMSS, CAS (China)

jcheng@amss.ac.cn

## Abstract

In both theory and practice, dealing with multiple zeros and clusters of zeroes or components with positive dimension of multivariate polynomial system is a challenging problem. We give a theoretical result to the problem. In fact, the idea of the main result comes from computer algebra systems. Based on some results related to computer algebra, we prove the main result (Theorem 1). Theorem 2 can be used with constructing roadmaps of a connected real component of a polynomial system. The symbolic computation based results may be a guide for numeric computation.

Denote  $\Sigma = \{f_1, \dots, f_m\} \subset \mathbb{R}[x_1, \dots, x_n]$ ,  $f = \sum_{i=1}^m f_i^2$ ,  $\mathfrak{S}_f = \{c \in \mathbb{C} : f - c \text{ is singular}\}$ ,  $\Sigma_r = \{\frac{\partial f}{\partial x_1}, \dots, \frac{\partial f}{\partial x_n}, f - r\}$ , where  $\mathbb{R}, \mathbb{C}$  are fields of real and complex numbers respectively.

**Definition 1** We say a point  $P$  is attracted to a component  $Q$  of  $V_{\mathbb{R}}(\Sigma_{\bar{r}})$  ( $\bar{r} \in \mathfrak{S}_f$ ) when  $r \rightarrow \bar{r}$  (simply for  $P$  is attracted to a component  $Q$  without misunderstanding) if there exists a path  $C$  from  $P$  to a point  $P' \in Q$  such that the value of  $r = f$  at point  $R \in C$  decreases to  $\bar{r}$  when  $R$  moves from  $P$  to  $P'$ .

We give a new criterion for numerically deciding whether a real point  $P \in \mathbb{R}^n$  is attracted to a real zero (regular, multiple or a point on a component with positive dimension) of a polynomial system.

**Theorem 1** Let  $\Sigma = \{f_1, \dots, f_m\} \subset \mathbb{R}[x_1, \dots, x_n]$ . Then there exists a real number  $r_0 > 0$  such that for any  $P \in \mathbb{R}^n$ , if

$$f(P) = \sum_{i=1}^m f_i^2(P) < r_0,$$

then  $P$  is attracted to a component of  $V_{\mathbb{R}}(\Sigma) \neq \emptyset$ .

Given two points  $P, Q \in \mathbb{R}^n$  that are attracted to some real zeros of  $\Sigma$ , we give a criterion to judge whether both  $P, Q$  are attracted to the same real connected component of  $\Sigma$ .

**Theorem 2** Let  $\Sigma = \{f_1, \dots, f_m\} \subset \mathbb{R}[x_1, \dots, x_n]$ . Let  $P_1, P_2 \in \mathbb{R}^n$  be two points and  $f(P_i) < r_0$  ( $i = 1, 2$ ), where  $f = \sum_{i=1}^m f_i^2$ . They are both attracted to the same component of  $V_{\mathbb{R}}(\Sigma)$  if and only if there exists a path  $C(P_1 P_2)$  such that for any point  $P$  on  $C(P_1 P_2)$ ,

$$f(P) \leq \max\{f(P_1), f(P_2)\}.$$

## Keywords

polynomial system, real zeros, certified numerical solving

# Planar arrangements and singular algebraic surfaces.

Juan García Escudero  
Universidad de Oviedo (Spain)

`jjge@uniovi.es`

## Abstract

Simplicial arrangements of lines have been used in the past decades to generate substitution tilings. They contain simple arrangements with a large number of triangular cells. Algebraic surfaces with many singularities can be constructed with polynomials based on the arrangements, which are also related to a class of bivariate polynomials with complex coefficients. The existence of a high number of singularities is due to the fact that the polynomials have many critical points with few critical values, which are obtained with Mathematica computational tool. A degree-15 algebraic surface with many  $A_7$  singularities is constructed with the help of Belyi polynomials. The Singular computer algebra system is used in order to get an explicit expression for the surface.

## Keywords

Algebraic Surfaces, Arrangements, Singularities.

## 1 Introduction

Simplicial arrangements of  $d$  lines were used in [12] for the derivation of substitution tilings with odd symmetries greater than five and not divisible by three. The constructions were later extended, first for  $d$  multiple by three, and then for  $d$  even, with the purpose of generating tilings with all the symmetries ([4], and references within). In [5] it is shown that simplicial arrangements, which we denote by  $S_D^{2d}$  and  $S_C^{2d}$ , contain the simple arrangements  $\Sigma_1^d$  and  $\Sigma_2^d$  that can be used for the generation of algebraic surfaces with many real nodes. On the basis of the construction of real variants of Chmutov surfaces [2, 1] are  $\Sigma_1^d$ , which already appeared in [8]. Of particular interest in singularity theory are  $\Sigma_2^d$ , for  $d$  divisible by three, because the associated algebraic surfaces have more real nodes than those obtained with  $\Sigma_1^d$ .

In this work we first study several properties of the arrangements such as the existence of Gallai triangles or the problem of stretchability and then we discuss their use in the context of singular algebraic surfaces. In [8], simplicial arrangements of type  $S_D^d$  were used to analyze the problem of the existence of Gallai triangles. The authors showed that there are no Gallai triangles in  $S_D^d$  for  $d$  higher than 4 with  $d$  not 0 (mod 9). We treat this question in Section 2 by studying the simplicial arrangements  $S_C^d$  for  $d = 0$  (mod 9). In Section 3 it is shown that by adding certain pseudolines to  $\Sigma_2^d$ , we can get non-stretchable simple arrangements. Simplicial pseudoline arrangements appear also in the context of substitution tilings. They contain the prototiles and substitution rules of the classes of random tilings obtained in [3]. In Section 4 we consider the relationship between the simple arrangements  $\Sigma_2^d$  and the existence of algebraic surfaces of degree  $d$  with many singularities. We give an explicit construction of a degree-15 surface with a high number of real singularities of type  $A_7$ . Mathematica [14] and SINGULAR [9] computing tools are used.

## 2 Simplicial arrangements of lines

### 2.1 The arrangements $S_C^d$

Let  $A$  be an arrangement of  $d$  lines and let  $t_j(A)$  denote the number of vertices of multiplicity (number of lines of  $A$  incident to a vertex)  $j$ . If all the bounded cells are triangles then we say that  $A$  is simplicial. If  $t_j(A) = 0$  for  $j$  higher than 2, then it is said to be simple. The following

question is attributed in [8] to Erdős. Let us suppose that the arrangement has  $t_j(A) = 0$  for  $j$  higher than 3. Then does there exist a Gallai triangle, i.e. three lines from  $A$  such that their three intersection points have multiplicity 2, or not?

We denote by  $P(0)$  a fixed point in the circle with center  $C$ . For  $\alpha = m\pi/2d, d \in \mathbf{Z}, m \in \mathbf{Z}_{2d}$ , let  $P(\alpha)$  be the point obtained by rotating  $P(0)$  around  $C$ , with angle  $\alpha$ .

The lines in the arrangements are defined by  $(m, n)$  if they pass through the points  $P(m\pi/2d)$  and  $P(n\pi/2d)$ . The simplicial arrangement  $S_C^d$ , with cyclic symmetry for  $d = 3q$ , consists in the straight lines  $L_{2n}$ , defined by  $(2n, d + 4 - 4n) \in \mathbf{Z}_{2d} \times \mathbf{Z}_{2d}$ .

*Lemma 1.* The lines  $L_i, L_j, L_k$  in  $S_C^d$  are concurrent if and only if  $i + j + k = 4 \pmod{2d}$ .

*Proof.* Two lines  $(x_1, y_1), (x_2, y_2)$  are perpendicular if and only if  $x_2 - x_1 + y_2 - y_1 = d \pmod{2d}$ .  $L_{2n}$  is perpendicular to the lines  $(d + 3 - n + m, d + 1 - n - m), m \in \mathbf{Z}_{2d}$ . Given  $n_1, n_2$  we look for  $n_3$  such that  $L_{2n_3} \perp (2n_1, 2n_2)$ . In that case, the lines  $L_{2n_1}, L_{2n_2}, L_{2n_3}$  are the altitudes of the triangle  $P(n_1\pi/d)P(n_2\pi/d)P(n_3\pi/d)$  and hence they meet at one point. The solution of  $2n_1 = d + 3 - n_3 + m, 2n_2 = d + 1 - n_3 - m$  is  $m = n_1 - n_2 - 1$  and therefore  $2n_1 + 2n_2 + 2n_3 = 4 \pmod{2d}$ .

*Lemma 2.* For  $d=0 \pmod{9}$  the arrangements  $S_C^d$  have no Gallai triangles.

*Proof.* The multiplicity of  $L_i \cap L_j$  is 2 when  $2i + j = 4$  or  $2j + i = 4 \pmod{2d}$ . The Gallai triangles are formed by  $L_i, L_j, L_k$  when  $2i + j = 2j + k = 2k + i = 4 \pmod{2d}$ . In order to find a Gallai triangle for  $d = 3q$  we have to look for  $m \in \mathbf{Z}$  such that  $3i - 4 = 2mq$ , which is not possible when  $q = 3 \pmod{3}$ .

## 2.2 $S_C^d$ and substitution tilings

The prototiles (minimal set of tiles such that each tile in the tiling is congruent to one of those in the prototile set) for a wide class of tilings can be obtained from  $S_C^d$  [4]. A substitution or inflation rule determines how to replace each prototile with a patch of tiles. Iteration of the substitution rules gives, in the limit, a substitution tiling. The possible patches of tiles necessary for the derivation of the rules are included in the simplicial arrangements. However, in order to get the inflation rules for all the possible inflation factors a different type of simplicial arrangement is needed. For instance in the case  $d = 9$  the arrangement  $S_D^9$ , with dihedral symmetry, is formed by  $(2n, 9 - 4n) \in \mathbf{Z}_{18} \times \mathbf{Z}_{18}$ . It contains three of the seven prototiles appearing in  $S_C^9$ , and it is possible to get substitution tilings with them [6]. For any positive integer  $q$ ,  $S_D^{3q}$  can be obtained by rotations of the lines in  $S_C^{3q}$ , as indicated at the end of section 4.1.

## 3 Simple and simplicial pseudoline arrangements

### 3.1 Non-stretchable simple pseudoline arrangements

The arrangement  $\Sigma_2^d$  is formed by the lines  $L_{2n+1}$  defined by  $(2n + 1, d + 2 - 4n) \in \mathbf{Z}_{2d} \times \mathbf{Z}_{2d}$ .

*Lemma 3.* The arrangements  $\Sigma_2^d$  are simple.

*Proof.*  $L_{2n+1}$  is perpendicular to the lines  $(d + 2 - n + m, d + 1 - n - m), m \in \mathbf{Z}_{2d}$ . Now we look for  $n_3$  such that  $L_{2n_3+1} \perp (2n_1 + 1, 2n_2 + 1)$ . We have  $2n_1 + 1 = d + 2 - n_3 + m, 2n_2 + 1 = d + 1 - n_3 - m$ , therefore  $2n_1 + 2n_2 + 2n_3 = 1 \pmod{2d}$  and  $2m + 1 = 2(n_1 - n_2)$  which is not possible, hence all the points  $L_i \cap L_j$  in  $\Sigma_2^d$  have multiplicity 2.

We can use  $\Sigma_2^d$  for the construction of non-stretchable simple arrangements of pseudolines. According to the Pappus-Pascal theorem, if the points  $A_1, A_2, A_3$  are collinear, and the points  $B_1, B_2, B_3$  are collinear, and if  $C_i$  is the intersection-point of the lines  $A_j B_k$  and  $A_k B_j$  for  $i \neq j \neq k \neq i$  then  $C_1, C_2, C_3$  are collinear.

We add three pseudolines  $P_k, k = 1, 2, 3$  to  $\Sigma_2^{12}$  in order to get a non-stretchable simple arrangement of 15 pseudolines  $S_{15}$ . The pseudolines are defined with 14-tuples which give the consecutive

intersections on lines  $L_k$ , denoted by  $k$ , and the other pseudolines:  $P_1 : (P_3, 13, 11, 15, 9, 17, 7, 5, 19, P_2, 21, 3, 23, 1)$ ;  $P_2 : (15, 17, 19, 13, P_3, 11, 21, 23, 9, 1, 7, 3, 5, P_1)$ ;  $P_3 : (P_2, 21, 19, 23, 17, 1, 15, 13, 3, P_1, 5, 11, 9, 7)$ . The intersections  $L_1 \cap P_1, L_1 \cap P_2, L_1 \cap L_{11}, L_{11} \cap L_{17}, L_{17} \cap P_3, L_{17} \cap P_1$  are denoted by  $A_1, A_2, A_3, B_1, B_2, B_3$  respectively.

Assume that we found an arrangement of straight lines  $T_{15}$  isomorphic to  $S_{15}$ ; we shall denote the vertices of  $T_{15}$  by the same symbols as those of  $S_{15}$ . Let  $C_2$  denote the intersection of the lines  $A_3B_1$  and  $A_1B_3$  in  $T_{15}$  (or the corresponding pseudolines in  $S_{15}$ ). The intersection point of  $A_2B_1$  and  $A_1B_2$  must be in the zone between the two lines passing through  $A_2$  and the line  $A_3B_1$ . On the other hand  $C_1$  must be below the line  $A_1B_3C_2$ . But  $C_2, C_1, C_3$  can not be collinear, which contradicts the Pappus-Pascal theorem. This means that the arrangement is non-stretchable. Analogous arguments can be applied to other arrangements with  $3q$  pseudolines constructed in a similar way.

### 3.2 Simplicial pseudoline arrangements and substitution tilings

In [3] several types of random substitution tilings were generated. The prototiles and inflation rules can be obtained from simplicial pseudoline arrangements. Nine pseudolines are necessary for the arrangement corresponding to the hexagonal tilings, which has three triangular prototiles and two types of substitution rules. For octagonal tilings the arrangement has ten pseudolines containing four prototiles. There are also two different substitution rules which may be combined in order to obtain random tilings.

## 4 Singular algebraic surfaces

### 4.1 Bivariate polynomials associated with the simple arrangements $\Sigma_2^d$

For  $d = 3q, q = 1, 2, 3, \dots$ , a simple arrangement of the type  $\Sigma_2^d$  can be described by means of the lines  $L_{\nu,d}(x, y) = 0, \nu = 0, 1, \dots, d-1$  where

$$L_{\nu,d}(x, y) := -y - \left(\cos \frac{(6\nu+1)\pi}{3d} - x\right) \tan \frac{(6\nu+1)\pi}{6d} - \sin \frac{(6\nu+1)\pi}{3d} \quad (1)$$

We define polynomials based on  $\Sigma_2^{3q}$  as

$$J_{3q}^C(x, y) := 3^{\frac{1-(-1)^q}{4}} (-1)^{\lfloor \frac{q+3}{2} \rfloor} \prod_{\nu=0}^{3q-1} L_{\nu,3q}(x, y) \in \mathbf{R}[x, y] \quad (2)$$

They have only three different critical values: 0, -1, 8. We have  $S_C^{2d} = \Sigma_2^d \cup S_C^d$  and the number of maxima with critical value 8 is the number of triples  $(i, j, k)$  such that  $L_i, L_j, L_k$  in  $S_C^d$  are concurrent [5]. On the other hand the minima are located inside the triangular cells of  $\Sigma_2^d$ , and the points with critical value 0 are in the intersections of two lines in  $\Sigma_2^d$ . In order to simplify the expressions for the polynomials we can use the following

*Lemma 4.* The polynomials  $J_d^C(x, y)$ , expressed in the variables  $u = x + iy, v = u^* = x - iy$ , have the form  $J_d^C(u, v) = -1 + j_d^C(u, v) + j_d^{C*}(u, v)$ , with  $j_d^C(0, 0) = 0$ .

*Proof.* In terms of the new variables, the lines in eq.(1) have the form  $L_{\nu,d}(u, v) = a_{\nu,d}u + a_{\nu,d}^*v + b_{\nu,d} = 0$ , where

$$a_{\nu,d} = \frac{1}{2} \left( \tan \frac{\nu\pi}{6d} + i \right), b_{\nu,d} = -\frac{\sin \frac{\nu\pi}{2d}}{\cos \frac{\nu\pi}{6d}} \quad (3)$$

We have  $L_{1,d}(u, v)L_{2,d}(u, v) = b_1b_2 + j_2^C(u, v) + j_2^{C*}(u, v)$  and, by induction on  $d$ ,

$$\prod_{\nu=0}^{d-1} L_{\nu,d}(u, v) = \prod_{\nu=0}^{d-1} b_{\nu,d} + j_d^C(u, v) + j_d^{C*}(u, v) \quad (4)$$

Now we want to prove that  $3^{\frac{1-(-1)^q}{4}}(-1)^{\lfloor \frac{q+3}{2} \rfloor} \prod_{\nu=0}^{3q-1} b_{\nu,3q} = -1$ . For  $q = 1, 2, 3, \dots$

$$\prod_{\nu=0}^{3q-1} \sin \frac{(6\nu+1)\pi}{6q} = (-1)^q \left( \prod_{\nu=0}^{q-1} \sin \frac{(6\nu+1)\pi}{6q} \right)^3 = (-1)^q 2^{-3q} i^{-3q} e^{i \frac{(2-3q)\pi}{2}} \left( \prod_{\nu=0}^{q-1} (e^{i \frac{(6\nu+1)\pi}{3q}} - 1) \right)^3 \quad (5)$$

If  $z_k$  denotes the roots of  $P(z) = (z+1)^q - e^{i \frac{\pi}{3}}$ , then  $\prod_{\nu=0}^{q-1} (e^{i \frac{(6\nu+1)\pi}{3q}} - 1) = \prod_{\nu=0}^{q-1} z_k = (-1)^q (1 - e^{i \frac{\pi}{3}})$ , therefore

$$\prod_{\nu=0}^{3q-1} \sin \frac{(6\nu+1)\pi}{6q} = \frac{(-1)^q}{2^{3q}} \quad (6)$$

The result of the lemma follows if we have in mind

$$\prod_{\nu=0}^{3q-1} \cos \frac{(6\nu+1)\pi}{18q} = 2^{-3q} e^{i \frac{(2-9q)\pi}{6}} \prod_{\nu=0}^{3q-1} (e^{i \frac{(6\nu+1)\pi}{9q}} + 1) = \frac{(-1)^{\lfloor \frac{q+1}{2} \rfloor} 3^{\frac{1-(-1)^q}{4}}}{2^{3q}} \quad (7)$$

where we have used the products of the roots of  $P(z) = (z-1)^{3q} - e^{i \frac{\pi}{3}}$ .

By applying eq.(7) we see also that the polynomial in eq.(2) corresponds to  $\tau = 0$  in  $J_{3q}(x, y, \tau) := -\prod_{\nu=0}^{3q-1} M_{\nu,q}(x, y, \tau)$ , where

$$M_{\nu,q}(x, y, \tau) := x \sin\left(\frac{(6\nu+1)\pi}{18q} + \tau\right) - y \cos\left(\frac{(6\nu+1)\pi}{18q} + \tau\right) - 2 \sin\left(\frac{(6\nu+1)\pi}{6q} + \tau\right) \quad (8)$$

For certain fixed values of  $\tau$ , the set of lines  $M_{\nu,q}(x, y, \tau) = 0, \nu = 0, 1, \dots, 3q-1$ , produces arrangements equivalent to  $\Sigma_1^{3q}, \Sigma_2^{3q}, S_D^{3q}, S_C^{3q}$  (see [6] for some examples). The so-called folding polynomials, associated with simple arrangements  $\Sigma_1^{3q}$  having one less triangle than  $\Sigma_2^{3q}$ , appear for  $\tau = \frac{4\pi}{3q}$ . As we have mentioned in Sec.2, the simplicial arrangements  $S_D^{3q}$  are necessary in order to get the inflation rules for the substitution tilings with the prototiles appearing in  $S_C^{3q}$ , whereas they contain enough information for the derivation of some tilings with less prototiles [6].

## 4.2 A degree-15 surface having many $A_7$ -singularities.

The polynomial in Lemma 4 for  $d = 15$  is

$$\begin{aligned} j_{15}^C(u, v) &= (50 - 125b)u^3 - (15 + 125b)u^6 - 75bu^9 - 15bu^{12} - bu^{15} + \frac{75}{2}uv - (225 - 750b)u^4v \\ &+ (15 + 525b)u^7v + 165bu^{10}v + 15bu^{13}v - 225u^2v^2 + (315 - 1575b)u^5v^2 - 675bu^8v^2 - 90bu^{11}v^2 \\ &+ 525u^3v^3 - (140 - 1400b)u^6v^3 + 275bu^9v^3 - 525u^4v^4 - 450bu^7v^4 + 189u^5v^5, \end{aligned}$$

with  $b = e^{-i \frac{\pi}{3}}$ . An  $A_j$ -singularity on a surface has the local equation  $z^{j+1} \pm x^2 \pm y^2 = 0$ . The real polynomial  $J_{15}^C(x, y)$ , which has coefficients in the algebraic number field  $\mathbf{Q}(\sqrt{3})$ , has one non degenerated minimum with critical value  $-1$  inside each of the 61 triangles in  $\Sigma_2^{15}$  and its critical points with critical value 0 correspond to the  $\binom{15}{2}$  points of intersection of the lines in  $\Sigma_2^{15}$ . On the other hand the Chebyshev polynomial  $(J_{15}^C(z, 0) + 1)/4$  has seven critical points with critical value 0 and also seven points with critical value 1. The surface  $J_{15}^C(x, y) + (J_{15}^C(z, 0) + 1)/4 = 0$  has  $7 \times \binom{15}{2} + 61 \times 7 = 1162$  real  $A_1$ -singularities, namely, seven more than the real variant of the Chmutov surface with the same degree [1]. This result can be checked also by employing the computational algebra system SINGULAR as in [7].

In [11, 7] Belyi polynomials were used with the purpose of obtaining hypersurfaces with many  $A_j$ -singularities. Now we construct a degree-15 surface having many  $A_7$ -singularities. It has the affine equation  $J_{15}^C(x, y) + (B_{15}^7(z) + 1)/2 = 0$ , where  $B_{15}^7(z)$  is a Belyi polynomial having two critical points with multiplicity 7. We define  $B_{15}^7(z)$  in such a way that  $\frac{dB_{15}^7(z)}{dz} = (z-a)^7(z-b)^7$ , with  $B_{15}^7(a) = 1, B_{15}^7(b) = -1$ . We can get an explicit expression for it by using Groebner basis, which in this case has two elements  $GI_1, GI_2$ . By using SINGULAR we obtain that  $GI_1 = GI_1(b), GI_2 = GI_2(a, b)$  have degrees 225 and 211. A factor of  $GI_1$  is  $g(z) = -6435 + 2048b^{15}$ . If we take the real root of  $g(z)$ , then  $a = -b$  and we find a solution for  $B_{15}^7(z)$  with real coefficients. The surface  $J_{15}^C(x, y) + (B_{15}^7(z) + 1)/2 = 0$ , where the normalized Belyi polynomial is

$$\frac{1}{26357760}(13178880 - 2^{11/15}3^{13/15}715^{14/15}19305z + 2^{1/5}3^{3/5}715^{4/5}180180z^3 - 3^{1/3}1430^{2/3}648648z^5 + 2^{2/15}3^{1/15}715^{8/15}3088800z^7 - 2^{3/5}3^{4/5}715^{2/5}1601600z^9 + 2^{1/15}3^{8/15}715^{4/15}3144960z^{11} - 2^{8/15}3^{4/15}715^{2/15}1774080z^{13} + 878592z^{15}),$$

has  $\binom{15}{2}+61=166$  real singularities of type  $A_7$ . This surface has one more  $A_7$ -singularity than the one studied in [11].

*Proposition 5.* If  $\mu_{A_j}(d)$  denotes the maximum possible number of  $A_j$ -singularities on an algebraic surface of degree  $d$ , then  $\mu_{A_7}(15) \geq 166$ .

In order to improve the known lower bounds for  $\mu_{A_j}(d)$ , simple arrangements containing the maximum possible number of triangles can be of interest. The following is a maximal simple arrangement with 7 lines and 11 triangles:  $(1, 5), (1, 7), (2, 10), (4, 10), (4, 12), (7, 13), (11, 13) \in \mathbf{Z}_{14} \times \mathbf{Z}_{14}$ . A maximal arrangement with 15 lines and 65 triangles is:  $(1 + 9n, 24 + 9n), (3 + 9n, 16 + 9n), (6 + 9n, 25 + 9n) \in \mathbf{Z}_{45} \times \mathbf{Z}_{45}$ ,  $n = 0, 1, 2, 3, 4$  (according to [10] the first one with 65 triangles was obtained in [13]). However, these particular maximal arrangements can not be used to improve the known lower bounds, because the corresponding polynomials do not have the same extreme values in all the critical points with critical value of the same sign. The results presented in this work suggest that if the cells appearing in the arrangements are prototiles of substitution tilings, then the polynomials which consist of the lines in the arrangements have few critical values. The construction of surfaces with many singularities can be based on such polynomials.

## References

- [1] S.Breske, O.Labs, D. van Straten, *Real line arrangements and surfaces with many real nodes*. In Geometric modeling and algebraic geometry. Springer. Berlin. (2008) 47-54.
- [2] S.V.Chmutov, *Examples of projective surfaces with many singularities*. J.Algebr.Geom. **1** (1992) 191-196.
- [3] J.G.Escudero, *Configurational entropy for stone-inflation hexagonal and octagonal patterns*. Int.J.Mod.Phys.B. **18** (2004) 1595-1602.
- [4] J.G.Escudero, *Random tilings of spherical 3-manifolds*. J.Gem.Phys. **58** (2008) 1451-1464.
- [5] J.G.Escudero, *A construction of algebraic surfaces with many real nodes*. <http://arxiv.org/abs/1107.3401> (2011).
- [6] J.G.Escudero, *Substitutions with vanishing rotationally invariant first cohomology*. Discrete Dyn. Nat. Soc. Article ID 818549, 15 p. (2012)
- [7] J.G.Escudero, *Hypersurfaces with many  $A_j$ -singularities: Explicit constructions*. J.Comput.Appl.Math. (2013), <http://dx.doi.org/10.1016/j.cam.2013.03.045>.
- [8] Z.Füredi and I.Palästi, *Arrangements of lines with a large number of triangles*. Proc.Amer.Math.Soc. **92** (1984) 561-566.
- [9] G.M. Greuel, G. Pfister *A SINGULAR introduction to commutative algebra*. Springer. Berlin. (2008).
- [10] B.Grünbaum, *Arrangements and Spreads*. American Mathematical Society. Providence. RI. (1972).
- [11] O.Labs, *Dessins d'enfants and hypersurfaces with many  $A_j$ -singularities*. J.Lond.Math.Soc. II.Ser.**74** (2006) 607-622.
- [12] K.P.Nischke, L.Danzer, *A construction of inflation rules based on n-fold symmetry*. Discrete Comput.Geom. **15** (1996) 221-236.
- [13] G.J.Simmons, *A maximal arrangement of sixteen lines in the projective plane*. Period.Math.Hung. **4** (1973) 21-23.
- [14] S.Wolfram, *Mathematica*. Addison-Wesley Publishing Co. (1991)



# Computations of Gröbner-Shirshov Basis and Reduced Words for Affine Weyl Group $\widetilde{A}_n$ using Mathematica

Erol Yılmaz, Cenap Özel, Uğur Ustaoglu  
Abant İzzet Baysal University (Turkey)

yilmaz\_e2@ibu.edu.tr

## Abstract

Gröbner and Gröbner-Shirshov bases theories are generating increasing interest because of its usefulness in providing computational tools and in giving algebraical structures which are applicable to a wide range of problems in mathematics, science, engineering, and computer science. In particular, Gröbner and Gröbner-Shirshov bases theories are powerful tools to deal with the normal form, word problem, embedding problem, extensions of algebras, Hilbert series, etc. The true significance of Gröbner-Shirshov bases is the fact that they can be computed.

Gröbner-Shirshov basis and normal form of the elements were already found for the Coxeter groups of type  $A_n, B_n$  and  $D_n$  in [1]. They also proposed a conjecture for the general form of Gröbner-Shirshov bases for all Coxeter groups. In [2], the example was given to show that the conjecture is not true in general. The Gröbner-Shirshov bases of the other finite Coxeter groups are given in [3] and [4]. This paper is the first example of finding Gröbner-Shirshov bases for an infinite Coxeter group, defined by generators and defining relations.

The main purpose of this paper is to find a Gröbner-Shirshov basis and as an application classify all reduced words for the affine Weyl group  $\widetilde{A}_n$ . The strategy for solving the problem is as follows:

Even though Gröbner bases algorithms implemented in Computer Algebra systems, there is no good Computer Algebra package to compute Gröbner-Shirshov bases. Because of non-commutative structure, it is not easy to find Gröbner-Shirshov bases. We wrote a program in Mathematica to find Gröbner-Shirshov basis of  $\widetilde{A}_n$  for small  $n$ 's. Then we generalize this set to any positive integer  $n$ , called it  $R'$ . After that using the algorithm of elimination of leading words with respect to the polynomials in  $R'$ , all the words in the group  $\widetilde{A}_n$  are reduced to the explicit classes of words for small  $n$ 's with help of Mathematica. As before, we also generalize this reduced set to any positive integer  $n$ . Then using combinatorial techniques, we compute the number of all reduced words with respect to these classes by means of a generating function. This generating function turns out to be same with the well known Poincaré polynomial of the affine Weyl group  $\widetilde{A}_n$ . Therefore, by the Composition-Diamond Lemma the functions in  $R'$  form a Gröbner-Shirshov basis for the affine Weyl group  $\widetilde{A}_n$ . Furthermore, one can easily see that this basis is in fact a reduced Gröbner-Shirshov basis.

## Keywords

Affine Weyl Groups, Gröbner-Shirshov Basis, Composition-Diamond Lemma, q-binomials

## References

- [1] L.A. Bokut and L.S. Shiao, *Gröbner-Shirshov bases for Coxeter groups*, Comm. Algebra **29** (2001), 4305–4319.
- [2] Y.Chen and C. Liu, *Gröbner-Shirshov bases for Coxeter groups I*, arXiv:0910.0096v1.
- [3] D. Lee, *Gröbner-Shirshov bases and normal forms for the coxeter groups  $E_6$  and  $E_7$* , Advances in Algebra and Combinatorics, World Scientific, 2008, 243–255.
- [4] O. Svechkarenko, *Gröbner-Shirshov bases for the Coxeter group  $E_8$* , Master Thesis, Novosibirsk State University, (2007).



---

---

# Session 1: Computer Algebra in Education

---

---

**Organizers:**

Michel Beaudin  
Michael Wester  
José Luis Galán García  
Alkis Akritas  
Bill Pletsch  
Elena Varbanova



# CAS: A Tool for Improving Autonomous Work

Alfonsa García, Francisco García  
Technical University of Madrid (Spain)

Ángel Martín del Rey, Gerardo Rodríguez  
University of Salamanca (Spain)

Agustín de la Villa  
Technical University of Madrid & Pontificia Comillas University (Spain)

avilla@upco.es

## Abstract

The EHEA proposes a student-centered teaching model. Therefore, it seems necessary to actively involve the students in the teaching-learning process. Increasing the active participation of the students is not always easy in mathematical topics, since, when the students just enter the University, their ability to carry out autonomous mathematical work is scarce.

In this paper we present some experiences related with the use of Computer Algebra Systems (CAS). All the experiences are designed in order to develop some mathematical competencies and mainly self-learning, the use of technology and team-work. The experiences include some teachers' proposals including: small projects to be executed in small groups, participation in competitions, the design of different CAS-Toolboxes, etc.

The results obtained in the experiences, carried out with different groups of students from different engineering studies at different universities, makes us slightly optimistic about the educational value of the model.

## Keywords

Autonomous work, Computer Algebra Systems, Engineering studies, Participation in competitions, Small projects, Toolboxes

# Assessing Mathematical Content in a Technology Environment

## Discussion Panel

A. Homero Flores  
Colegio de Ciencias y Humanidades-UNAM, México

ahfs@unam.mx

### Abstract

It seems that teaching and assessment are two independent aspects of the educational process. At least that is the trend in the past years. While teaching is left almost entirely to classroom teachers, assessment is mostly a matter of school districts and governments.

Teachers teach with the support of textbooks and teaching activities, and assessment is made mostly with tests and examinations.

In an educational context, assessment has always been attached to the process of grading, and test, exams or questionnaires are the main assessment tool. But currently, there is an overestimation of this tool, as some journalist points out in the next quote:

Tests have always been a part of teaching, traditionally used as just one means of evaluating students' progress along the long, curving path of learning as well as a means of documenting their outcomes at the end of a teaching cycle. What's different in today's test-obsessed educational culture is the increasing frequency and prevalence of high-stakes exams as a primary tool of assessment and the decreasing autonomy teachers have over what skills and knowledge get measured and how. [http://www.lcsun-news.com/las\\_cruces-opinion/ci\\_22859295/their-view-educational-testing-new-march-madness](http://www.lcsun-news.com/las_cruces-opinion/ci_22859295/their-view-educational-testing-new-march-madness) (recovered March 30, 2013).

Besides, assessment always (or almost always) has been on students performance, knowledge and skills. For instance take a look to what the American Psychology Association says about tests:

Today, many school districts are mandating tests to measure student performance and to hold individual schools and school systems accountable for that performance. Knowing if and what students are learning is important. Test results give classroom teachers important information on how well individual students are learning and provide feedback to the teachers themselves on their teaching methods and curriculum materials. It is important to remember, however, that no test is valid for all purposes. Indeed, tests vary in their intended uses and in their ability to provide meaningful assessments of student learning. Therefore, while the goal of using large-scale testing to measure and improve student and school system performance is laudable, it is also critical that such tests are sound, are scored properly, and are used appropriately. <http://www.apa.org/pubs/info/brochures/testing.aspx> (recovered March 30, 2013).

This regarding of tests as the one and only assessment tool is affecting the way and goal of teaching in basic education, as one high school teacher in Slovenia commented in a Mathematics Education Course given in Ljubljana: *"Yes, this methodology of learning mathematics, doing mathematics is alright, but I find it hard to implement here in Slovenia because that way of teaching is slow and takes time, and we have a very heavy curriculum and our students must score well in 'matura' (state tests), so the best we can do is to prepare pupils for 'matura' "*

In the USA, for instance, high stake testing is becoming a nuisance for students, teachers and school authorities. For instance, it is relevant to take a look to the webpage of The National Center for Fair and Open Testing.

One of the aspects of this is the growing cases of cheating in tests, the more relevant case being the one of Atlanta:

<http://www.fairtest.org/2013-Cheating-Report-PressRelease> (Recovered March 30, 2013).

The other one is how low scores in standardized testing is affecting teachers and school performance and financial bonuses (<http://www.fairtest.org/k-12/teachers>, recovered March 30, 2013).

The reaction to this kind of problems is an increasing reject of high stake tests by teachers, parents and administrators (<http://www.fairtest.org/k-12/high%20stakes>, recovered 30 March, 2013).

And in many countries, PISA scores, a mere indicator as how is the state of education, is becoming an ultimate goal for education systems, instead of acquisition of knowledge.

Mathematics education is not the exception to the rule.

One way of overcoming these problems -or at least to avoid some of the problematic aspects of high stake testing- is to focus our attention in the classroom. Assessment can be done inside the classroom (formative assessment), and outside the classroom (school system evaluation); and it could be a close relationship between the two.

On one hand, standardized exams is the only way government educational offices and international organizations (as OECD or UNESCO) have in order to measure students performance and state of educational systems, this kind of assessment is done outside the classroom by agents not directly involved in the teaching-learning process as teachers and students do; on the other, formative assessment is the way teachers and students have in order to measure their performance and development in learning tasks and their acquisition of knowledge inside the classroom.

What I call classroom assessment should be the way to improve teaching-learning processes; and outside evaluation (standardized testing made outside the classroom) would be the gauge to measure the acquisition of knowledge and skills in schools.

Traditionally, the teaching process has been classified in three stages: planning, applying, and assessing. In general, assessment is made by way of tests or examinations in order to get information about students previous knowledge and skills, and about the ones acquired during the teaching-learning process. But almost always, tests and questionnaires are given at the end of a teaching cycle -call it teaching unit, course or semester-, and almost always its only function is to gather evidences of the note the student has got. In the educational literature this is called summative assessment.

So, we understand classroom assessment as the gathering of information to feedback and improve the teaching and learning of any content matter. In order to be effective it should be an integral part of the teaching methodology and not a separate issue ([1]). That is, the teaching-learning process should take place in an environment of classroom assessment; this concept is close to the concept of formative assessment.

Took in this way, assessment should be a continuous process in which teaching and learning is embedded, and it could be used as well to give a note to the student at the end of the course, i.e. students grading is only a tiny part of assessment.

In what Mathematics Education is concerned, as well as in the teaching and learning of science and engineering, the use of technology is widely spread in classrooms; manly CAS and DG software, and Information and Computer Technology (ICT).

With the use of technology in the teaching of mathematics people rises the question on how to have an assessment that takes into account the technological aspect of the process. We claim that it is not necessary to be concerned about this: The relevant issue on the use of technology, besides its capacity to foster problem-solving skills and to develop mathematical thinking, is its potential use as an assessment tool itself. That is, technology, particularly mathematics teaching technology, could be a window toward students knowledge and attitudes in the sense of [2].

Lets see for instance, if we ask our students to construct a square using only paper and pencil and look at the figures, we are going to see more or less good drawings of squares, but no more information about the knowledge of the student on the issue; in the other end of the situation, if we ask students to construct a square in three different ways using a DG Software, depending on the construction we are going to have a lot more information about the concept of square the student knows and, besides, on the use of the software.

The discussion panel will discuss assessment and educational technology in this context and the objective would be to jump into some preliminary conclusions and lay the basis for further discussions and research projects.

Some of the questions that will trigger the discussion are:

- Should we use the same assessment tools as questionnaires and tests to assess technology based teaching activities or we should look for different assessment tools?
- How can we observe the knowledge that a student puts into play when is using technology in mathematical tasks?
- Is this knowledge the same regardless the technology, for instance a DG software or a CAS software?

- We need to assess the use of technology on everyday classroom or should we use technology as an assessment tool by itself?

The structure of the panel would be as follows:

1. The panel is one hour in duration
2. It is proposed at most three panelists. Each one should have a ten minutes presentation addressing one or several of the discussion questions posed above. (30 minutes)
3. After this, we open the session to the opinions and commentaries of the audience (15 minutes).
4. Finally, each panelist should have 5 more minutes in order to closed his/her intervention and propose some further discussion.
5. The panel should have a coordinator who organizes the discussion.

Note: The proposal of this Discussion Panel is part of the Infocab Project PB101213.

### **Keywords**

Classroom assessment; Standardized tests; CAS and DG technology

## **References**

- [1] Flores, H. and Gomez, A. (2009). Aprender Matemática, Haciendo Matemática: la evaluación en el aula. Educación Matemática, vol. 21, núm. 2, pp. 117-142.
- [2] Noss, R. and Hoyles, C. (1996). Windows on Mathematical Meanings: Learning Cultures and Computers. Dordrecht: Kluwer Academic Publishers.



# Global application of CAS tools for teaching in Computer Engineering degrees

S. Cárdenas, I. Fortes, I. Pérez de Guzmán, S. Sánchez, A. Valverde  
University of Málaga (Spain)

`ifortes@uma.es`

## **Abstract**

In Engineering degrees, the use of CAS tools must be integrated as an educational tool that will have a professional use in the future, that is, they have to be something more than class usage within a subject. In this paper, we present the experiences of a group of teachers of the Applied Mathematics area at Málaga University teaching in Computer and Engineering degrees. An integral program of training, use and creation of free software of Mathematics for the students is developed. CAS tools are used in the subjects of the first course as habitual tool of work. The formation in CAS is carried out by means of a on-line subject that introduces the basic managing of several programs of Mathematics (Maxima, Octave, SciLab, R, Sage, Geogebra, ...). Some advanced applications of the use of these programs are introduced in the subjects. Also, the creation of open sources software and development of CAS tools for complete applications or modules for other programs are developed (development of routines of symbolic calculation, cross-platform environments, web for free software, applications for mobile devices, ...).

## **Keywords**

CAS tools, on-line training, open sources software

# In praise of rectangular systems

David Jeffrey  
University of Western Ontario, London, Canada

djeffrey@uwo.ca

## **Abstract**

Most linear algebra courses teach the subject concentrating on square systems of equations (number unknowns = number equations).

In this paper, I argue that this emphasis is wrong and we should teach the subject discussing rectangular systems. This is particularly appropriate for engineering students.

Computer Algebra systems allow us to analyse rectangular systems easily, and therefore allow us to teach this way. Examples from the author's lecture notes will be given.

## **Keywords**

Linear Algebra, Row reduction, Gaussian elimination, Determinants, over-determined systems

# Polynomial Systems Solving with Nspire CAS (Part I, Part II)

Michel Beaudin, Gilles Picard, Geneviève Savard  
École de technologie supérieure (Canada)

`gilles.picard@etsmtl.ca`

## Abstract

Nspire CAS can solve polynomial systems, using the Gröbner-Buchberger elimination method, but users don't have access to an explicit function like the one found in *Derive* (the so called "Groebner\_basis" function). Thus we cannot see how the method is used when solving polynomial systems with Nspire CAS. In this talk, we will show typical examples of polynomial systems that arise when teaching Lagrange multipliers technique. In the first part, the example will emphasise the importance of checking solutions and examining graphically the problem. The second example, in part two, will show a classic optimization problem where we will analyze the answer given by the commands "solve" and "zeros": we will find one wrong solution and some solutions will be missing (but simple parametric equations of the constraint will help us find the right answer). Using *Derive*'s Groebner\_basis function, we will try to show what can yield this problem.

When teaching row-reduce echelon form to students, we tell them that this is the way a linear system should be solved in general instead of constantly applying the (black box) "solve" command. In case of polynomial systems, access to a "Gröbner basis function" would be, for users, an important tool for understanding results obtained by the Nspire CAS system.

## Keywords

Polynomial systems, solving facilities, Lagrange multipliers, Gröbner basis.

# Some maths problems for the average citizen

Eugenio Roanes-Lozano  
Instituto de Matemática Interdisciplinar (IMI),  
Departamento de Álgebra, Facultad de Educación,  
Universidad Complutense de Madrid, E-28040 Madrid (Spain)

Justo Cabezas-Corchero  
High School Mathematics Professor (Ret.)  
Badajoz, Spain

`eroanes@mat.ucm.es`

## Abstract

We have been always surprised by the inability of many students to adequately treat some problems of everyday life that only require of elementary mathematics (meanwhile they can solve problems with a much more complicated background). Obviously, the reason is that they haven't been trained in facing these sorts of problems. We shall give an overview of some of the typical mathematical problems that an average citizen needs to know how to face. In most of them a CAS helps (avoiding the tedious computations), but cannot solve the problem by itself. But we believe that CAS can be key in the process of experimenting with these problems in order to achieve the necessary skills for solving them in real life.

## Keywords

Basic Mathematics, Curriculum, CAS

## 1 Introduction

The first author has taught at the School of Statistics, the School of Education and the School of Mathematics of the Universidad Complutense de Madrid for more than 25 years. His students have ranged from freshmen to Ph.D. students.

The second author has been a mathematics high school teacher for more than 35 years. He has also taught maths at different schools of the Universidad de Extremadura.

We have been always surprised by the inability of many students to adequately treat some problems of everyday life that only require elementary mathematics (meanwhile they can solve problems with a much more complicated background). Obviously the reason is that they haven't been trained in facing these sorts of problems.

An example is percentages. The first author is now teaching a subject entitled "Elementary mathematics with computer" to 2nd year pedagogy degree students (in it, elementary mathematical problems are treated using CAS and DGS). While most of these students could calculate a discount on a price, not all could correctly solve a similar problem: write a computer program that, given the total diameters of two tires, decides whether the new tire differs by more than 3 % w.r.t. the old one (the obstacle was mathematical, not computer related). Moreover, they were not sure if adding a tax plus a discount to a price (both expressed as percentages) did commute. Meanwhile, they use SPSS in complicated statistical studies regarding pedagogical issues.

In ancient cultures mathematical research was mainly focused on topics with a direct application: plane geometry (for surveying and architecture) and astronomy (for religious reasons and navigation), although this knowledge was not intended for the average citizen. But these interests have been changing in the last thousand years.

Many of the problems that could now be of "general interest" have an economical background, and many require the use of elementary physics (mainly physical units). Some examples can be found afterwards.

## 2 Some of the examples detected

Examples of some of the topics that we have detected that could be labeled as *important* for an average citizen (*essential skills*) follow. We have only included situations that we believe are not correctly covered (in practice) by the Spanish educational system.

### Economy:

- Do you save money if you change your present (perfectly working) refrigerator by an A++ one?
- According to your present telephone invoice, should you migrate to another company with a completely different way to bill the phone calls that looks much cheaper?
- Should you change your present car (in its midlife) by a much more ecological new hybrid for economical reasons?
- Are low consumption bulbs worth their higher price?

Nevertheless, there are many other mathematical topics related to real life situations. Some examples follow.

### Divisibility:

- My living room is  $5.40m \times 4.20m$  and I would like to cover the floor with tiles but I don't have a tile cutting machine. Which is the maximum tile size that I can use?

### Dilating areas and volumes and scales:

- This frustoconical drinking glass looks a bit too small. I'll buy this other one that is 1.3 times higher and wider. It is just a bit bigger than the other one, right?
- The rooms in this house floor plan look huge. Is the furniture represented in the house floor plan at the correct scale?

### Derivatives (or increments):

- I can find in a local newspaper that "Unemployment has decreased its growth" meanwhile another paper (of a different political tendency) publishes the same day that "Unemployment has grown". Can we be assured that at least one of them is lying?

### Combinatorics:

- In a certain lottery there are 100 numbers. The probability to win if I buy one day one number is 1%. If I buy a ticket today and a ticket tomorrow the probability to win is  $1\%+1\%=2\%$ . OK?

### Cardinal of the union / Probability of the union:

- In this class there is 45% males and 30% people from Andalusia. Do you agree that one way or another we cover 75% of the students?

### Negative exponential:

- Why should I take antibiotics (and many other drugs) following a strict dosage schedule?
- I know that Carbon-14 is an unstable isotope of Carbon, but how does Carbon-14 dating work?

### Correlation:

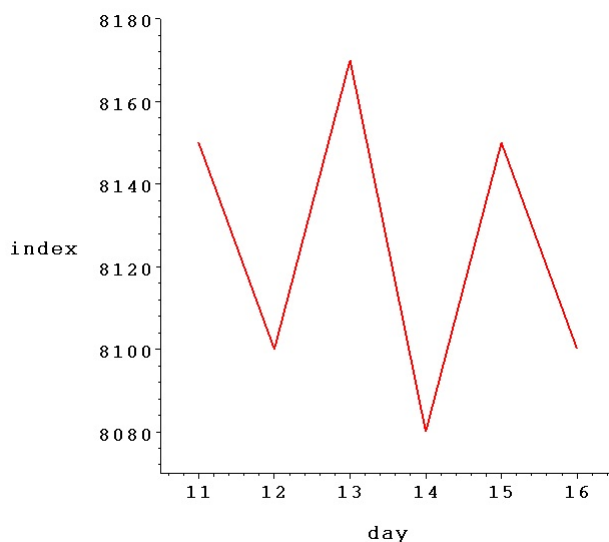
- There is no "functional relation" between the height and weight of people, but is there any other kind of "relation"?

### Normal distribution:

- How can shops decide which shoe sizes should they have in stock?
- For what range of student IQ is the curriculum designed?

### Interpretation of graphic representations:

- In the figure below the evolution of a certain stock exchange index along one week is represented. It reflects huge economical movements, doesn't it?



### Partial ordering:

- According to a Spanish saying: “All comparisons are obnoxious” (“Todas las comparaciones son odiosas”).

## 3 Remark

Once the first draft of this Extended Abstract was already prepared, one of the main Spanish newspapers published an impressive report about the failures in elementary mathematics (and other subjects) of students with a degree in Primary School Teaching during their competitive recruitment examinations in the Madrid region<sup>1</sup>. The exercise with the worst results (7.09% of the answers were correct) was an elementary example about time, weight and area unit conversion.

## 4 Conclusions

Taking into account that most citizens are not mathematicians, we believe that this sort of topics/problems, closer to everyday life, should be included into the curricula in order to provide a “more useful” mathematics education.

Moreover, the computations required by many of these problems can be bypassed using a CAS (a CAS can even carry units along with the computations).

An issue to be discussed is whether it would be better to treat these topics/problems within the traditional curricula or in separate workshops.

<sup>1</sup>Pilar Álvarez, Maestros suspensos en primaria (in Spanish). El País, March 13th 2013 [http://sociedad.elpais.com/sociedad/2013/03/13/actualidad/1363202478\\_209351.html](http://sociedad.elpais.com/sociedad/2013/03/13/actualidad/1363202478_209351.html).

Anonymous, Las matemáticas se resisten (in Spanish). El País, March 13th 2013. [http://sociedad.elpais.com/sociedad/2013/03/13/actualidad/1363201114\\_422663.html](http://sociedad.elpais.com/sociedad/2013/03/13/actualidad/1363201114_422663.html)

# Investigating Magic Squares in a Linear Algebra Course

Karsten Schmidt  
Schmalkalden University of Applied Sciences, Germany

kschmidt@fh-sm.de

## Abstract

A magic square of order  $n$  is a square arrangement of  $n^2$  real numbers, such that the sum of the elements in each row, column, and diagonal is equal to a constant  $s$ , its magic sum.

Let the  $n \times n$  matrix  $M$  denote a magic square, the  $n \times 1$  vector  $j$  the vector of ones, the  $n \times n$  matrix  $F$  the flip matrix, e.g. for  $n = 3$ :  $\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$ , and  $'$  transposition.

The following interesting activities can be carried out in class at very different stages of the course, using a Computer Algebra System like Derive to facilitate computations:

1. Computing the matrix product  $Mj$  and comparing it to the scalar product  $sj$  to check whether the  $n$  row sums are indeed equal to  $s$ .
2. Computing the matrix product  $j'M$  and comparing it to the scalar product  $sj'$  to check whether the  $n$  column sums are indeed equal to  $s$ .
3. Computing the trace of  $M$  to check whether the sum of the elements of the main diagonal is equal to  $s$ .
4. Computing the trace of  $FM$  (left multiplication by  $F$  reverses the rows of a matrix) to check whether the sum of the elements of the antidiagonal of  $M$  is equal to  $s$ .
5. Reconsidering the equation  $Mj = sj$  to realize that  $s$  is one of the eigenvalues, and  $j$  an associated eigenvector, of  $M$ .

Any  $3 \times 3$  magic square can be written as the sum of two matrices,  $M = sG + N$ , where  $G = \frac{1}{3}J$  ( $J = jj'$  denotes the  $3 \times 3$  matrix of ones), and  $N$  has a simple structure defined by only two real numbers as well. The matrices  $G$ ,  $N$ , and  $M$  provide good examples to compute the trace, determinant, rank, and eigenvalues, and investigate the connections between them.

A further interesting activity is to compute the inverse (if  $M$  is nonsingular), or Moore-Penrose inverse (if  $M$  is singular), of  $M$ , and investigate whether it is also magic. Again, the use of a CAS is essential in order to facilitate computations.

The famous Lo-Shu magic square  $\begin{pmatrix} 4 & 9 & 2 \\ 3 & 5 & 7 \\ 8 & 1 & 6 \end{pmatrix}$  will be one of the examples used throughout the presentation.

## Keywords

magic squares; eigenvalues; inverses

# Computer Algebra - the engine of transition to activity-based approach in mathematics education

Elena Varbanova, Elena Shoikova  
Technical University of Sofia (Bulgaria)

`elvar@tu-sofia.bg`

## **Abstract**

The paradigm of time-and-content based education gives nowadays way to the new paradigm of instruction-and-activity based education. The latter is a result of the widespread use of computer technologies. But are they oversold or underused in education? We still observe patchy implementation of these technologies in mathematics education. Computer technologies allow to introduce

- teaching strategies that aim to increase the autonomy of learners
- learning methodology that puts learner autonomy at its heart
- assessment strategies that interpret and use student achievement to make decision about the next steps in instruction.

The need of considering all the three components of the triad teaching-learning-assessment (TLA) in tandem and not focus on any one of them is discussed. The role of informed use of computer algebra in the TLA process is illustrated by means of appropriate applications. Authors' experience in developing instruction-and-activity based seminar and laboratory classes in calculus is shared. They support self-directed (independent) learning. Computer algebra systems serve as a knowledge and collaboration instrument not restricted to any particular didactical model.

## **Keywords**

Activity-based education, Mathematics with technology, Computer algebra, Calculus



# Using Computer Algebra in Mathematics for Engineers

Thomas Westermann  
University of Applied Sciences (Germany)

`thomas.westermann@hs-karlsruhe.de`

## Abstract

Computer algebra systems (CAS) have improved the mathematical work of engineers. The systems are used for numerical computations as well as for algebraic manipulations of equations. Moreover, the powerful graphical capabilities and the easy use of the graphics are applied to display complicated functions and technical results. The techniques in hand calculations are trusted into the background in favor of the systematic approach in mathematics and of the exciting modelling of realistic systems. This exciting aspect has been taken up and the CAS Maple was included in the education of engineers. Mathematical concepts are motivated in a clear and vivid manner by the use of the visualization and animation capabilities of Maple.

In this paper the principal concept and the application of Maple in engineering education will be demonstrated in various examples:

- Lengthy and abstract topics like the convergence of Fourier series to a given function are discussed.
- The visualization of the wave equation in case of a vibrating string is performed.
- Eigenvectors can be identified geometrically by showing an animation of a rotating vector.
- Finally, the oscillations of an idealized skyscraper are computed to visualize the meaning of eigenvalues and eigenvectors, physically.

For each of these examples a worksheet can be used interactively.

## Keywords

Mathematics for Engineers, Maple, Mathematical Concepts, Visualization

# Omega: A Free Computer Algebra System Explorer for Online Education

Michael Xue  
Vroom Laboratory for Advanced Computing (US)

mxue@vroomlab.com

## Abstract

Students and faculty have traditionally relied on handheld graphing calculators or using Computer Algebra System (CAS) installed in computer labs on campus. The ubiquitous online education has created a demand for an economical, ready online access to CAS.

In this presentation, we will introduce Omega, a free online CAS Explorer that provides user with immense power in both symbolic and numeric computing. To use Omega, only a web browser is required. User composes and submits mathematical query using a calculator-like graphical user interface. (see Fig. 1) Upon submission, the query is processed by Omega's CAS engine, Maxima, and the result is displayed in text or graphic formats. Using the built-in functions of the web browser, the output can be exported for further manipulation.

Omega can be accessed from desktop/laptop computers, ipad/tablets, and smartphones. It is compatible with all major web browsers. In addition to Maxima, other CAS can also be used as Omega's underlying engines.

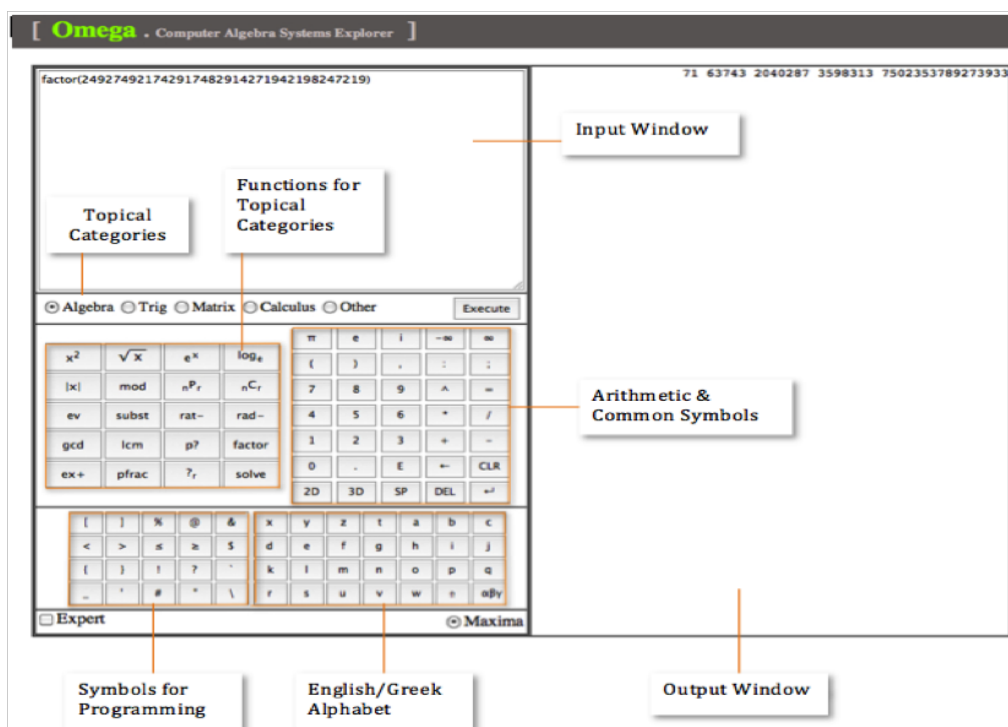


Fig. 1

Below screen shot (Fig. 2) illustrates step-by-step how to use Omega interface to solve a quadratic equation  $x^2 - x - 1 = 0$ .

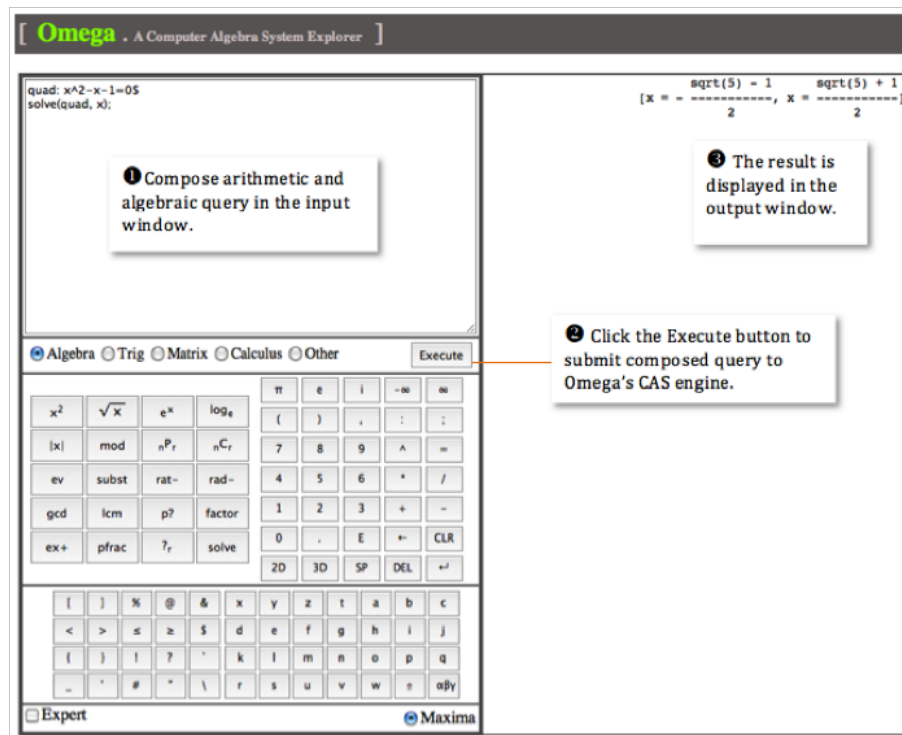


Fig. 2

Omega can visualize curves and surfaces via two dynamic plotting functions located on the arithmetic and common symbols keypad: (Fig. 3)

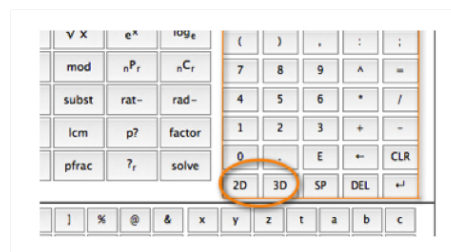


Fig. 3

The 2D plot function enters a default template in the input widow. The user can edit the functions and adjust the plotting range. The following example shows how to plot function  $x^2 - x - 1$  where  $x$  varies from -5 to 5: (Fig. 4)

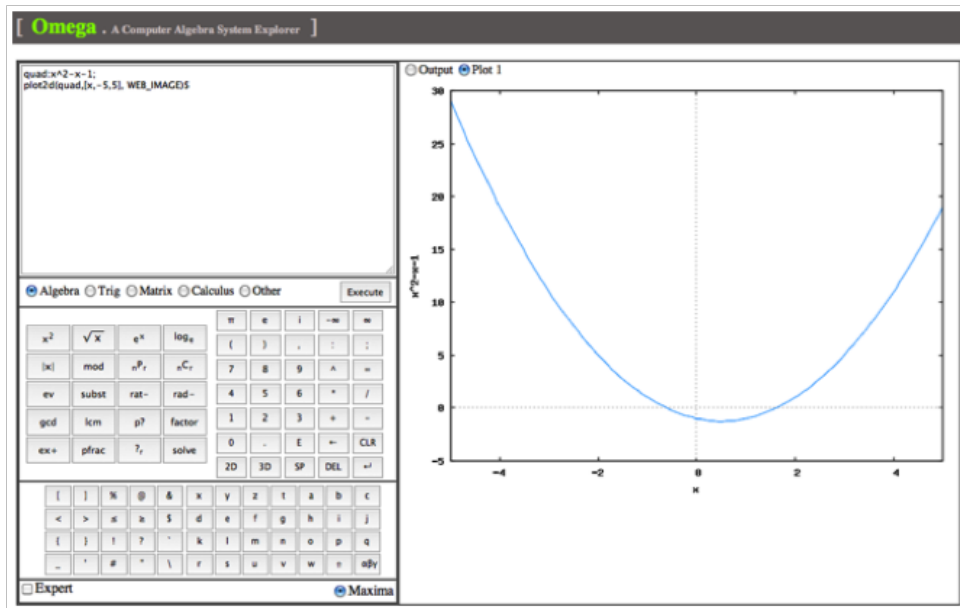


Fig. 4

3D plot function is similar to 2D plot function: (Fig. 5)

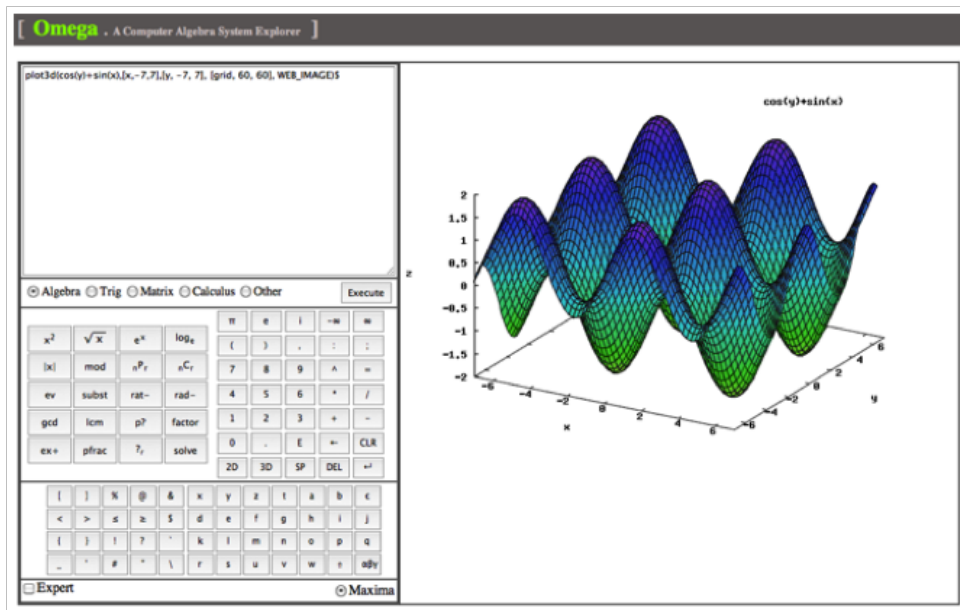


Fig. 5

Among advanced features, Omega incorporates powerful programming language in its functions. Program can be written in CAS engine-specific programming languages: (Fig. 6)

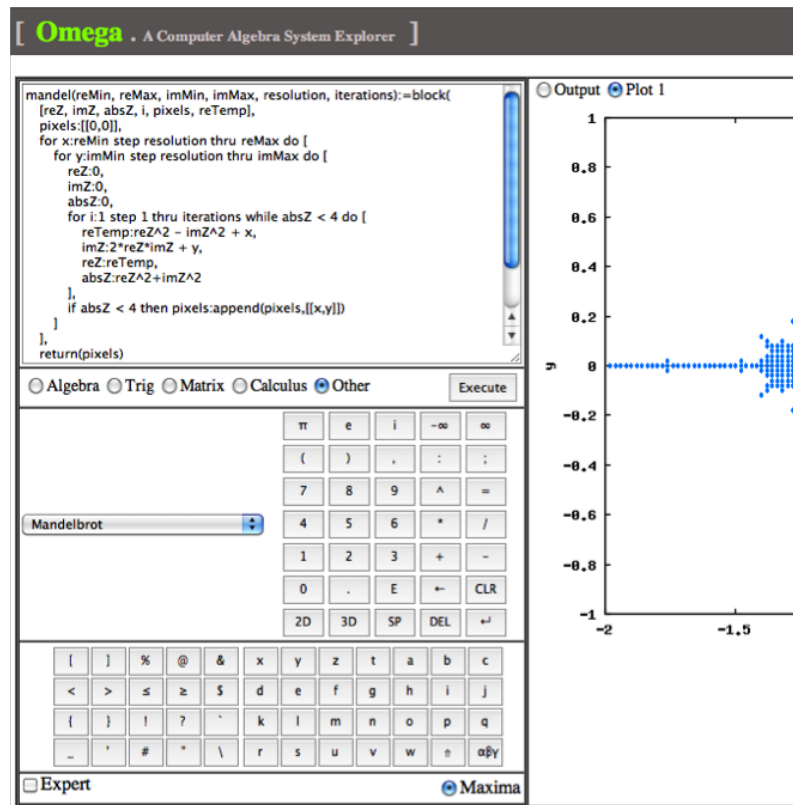


Fig. 6

Just-in-time Help for all function keys is a very important feature for CAS users. Omega function keys display mouse-over tool-tips description. (Fig. 7)

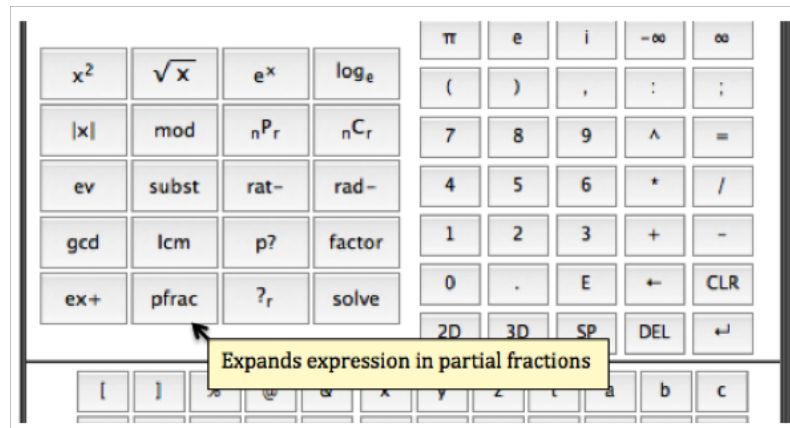


Fig. 7

Click on the function key will display just-in-time Help from the underlying CAS engine in the output window. The Help content provides specific descriptions of each function key, query composition syntax, and additional examples: (Fig. 8)

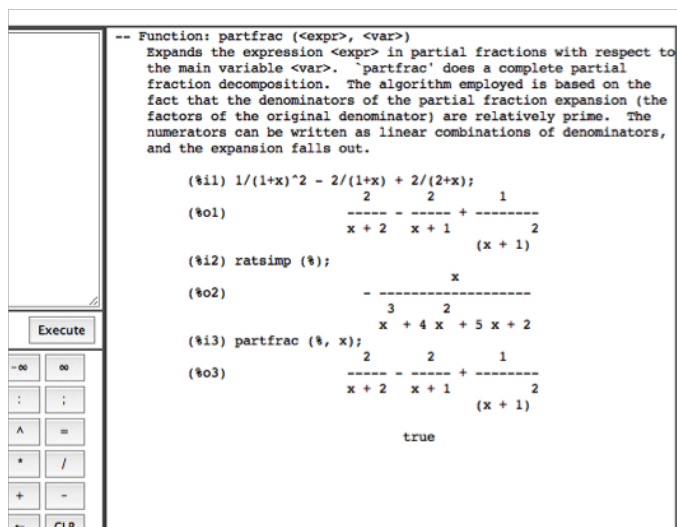





Fig. 8

Users familiar with the CAS can turn off just-in-time Help by checking the box next to the Expert option at the lower corner of the screen:



Fig. 9

The  button will turn into  after it is clicked, indicating computation is in progress. Click on  will terminate a running process.

## References

Maxima Documentation (<http://maxima.sourceforge.net>)

---

---

# Session 2: Computer Algebra for Dynamical Systems and Celestial Mechanics

---

---

Organizers:

Victor Edneral  
Aleksandr Myllari  
Valery Romanovski  
Nikolay Vassiliev





# On necessary conditions of integrability of degenerated planar ODE systems in the parameter space

Alexander Bruno

Keldysh Institute for Applied Mathematics of RAS (Russia)

Victor Edneral

Skobeltsyn Institute of Nuclear Physics  
Lomonosov Moscow State University (Russia)

`edneral@theory.sinp.msu.ru`

## Abstract

We consider an autonomous system of ordinary differential equations, which is resolved with respect to derivatives. To study local integrability of the system near a degenerate stationary point, we use an approach based on Power Geometry and on the computation of the resonant normal form. For the partial non Hamilton 5-parameter case of concrete planar system, we found the almost complete set of necessary conditions on parameters of the system for which the system is locally integrable near a degenerate stationary point. These sets of parameters, satisfying the conditions, consist of 4 two-parameter subsets in this 5-parameter space except 1 special hyper plane. We wrought down 4 the first integrals of motion as functions in parameters of the system. But we can say nothing about possibility an existence of additional first integrals at the single special values of one of the parameters.

## Keywords

Ordinary differential equations, Integrability, Resonant normal form, Computer algebra

# On Using of Computer Algebra Systems for Analysis of Rigid Body Dynamics

Larisa Burlakova, Valentiv Irtegov  
Institute of Systems Dynamics and Control Theory (Russia)

irteg@icc.ru

## Abstract

The paper presents some results of qualitative analysis of conservative systems. The modified Routh-Lyapunov technique is used as tool for investigation. Special attention is paid to algorithms of finding and analysis of invariant manifolds on which elements of algebra of problem's first integrals assume a stationary value.

## Keywords

first integrals, invariant manifolds, conservative system, stability

## Introduction

Application of modern tools of computer algebra (CA) allows one significantly to increase the number of effective algorithms which are used for qualitative analysis of dynamic systems. The paper discusses several algorithms which are some generalization of the Routh-Lyapunov technique [1] of analysis of conservative systems with algebraic first integrals. These algorithms are: the use of enveloping integral for family of first integrals in order to find invariant manifolds (IM) and to investigate their stability [2]; solving a system of stationary equations of a family of first integrals with respect to some part of phase variables and some part of parameters of family's first integrals [3]; finding IM of 2nd and higher level on earlier found IMs. Efficiency of these approaches is demonstrated by examples of analysis of two classical completely integrable systems.

## 1 Kovalevskaya's Case.

In Kovalevskaya's problem [4] of motion of a rigid body with a fixed point the equations of motion write

$$2\dot{p} = qr, \quad 2\dot{q} = -rp + x_0\gamma_3, \quad \dot{r} = -x_0\gamma_2, \quad \dot{\gamma}_1 = r\gamma_2 - q\gamma_3, \quad \dot{\gamma}_2 = p\gamma_3 - r\gamma_1, \quad \dot{\gamma}_3 = q\gamma_1 - p\gamma_2,$$

and have the following first integrals

$$2H = 2p^2 + 2q^2 + r^2 + 2x_0\gamma_1 = 2h, \quad V_1 = 2p\gamma_1 + 2q\gamma_2 + r\gamma_3 = m, \\ V_2 = (p^2 - q^2 - x_0\gamma_1)^2 + (2p q - x_0\gamma_2)^2 = k^2, \quad V_3 = \gamma_1^2 + \gamma_2^2 + \gamma_3^2 = 1.$$

Consider the problem of finding IMs on which Kovalevskaya's integral  $V_2$  assumes a stationary value. The necessary conditions of extremum for integral  $V_2$  have the form:

$$\frac{\partial V_2}{\partial p} = 4(py_1 + qy_2) = 0, \quad \frac{\partial V_2}{\partial \gamma_1} = -2x_0y_1 = 0, \quad \frac{\partial V_2}{\partial q} = -4(qy_1 - py_2) = 0, \quad \frac{\partial V_2}{\partial \gamma_2} = -2x_0y_2 = 0. \quad (1)$$

From equations (1), where the following denotations  $y_1 = p^2 - q^2 - x_0\gamma_1$ ,  $y_2 = 2p q - x_0\gamma_2$  were used, we conclude that the equations for one of invariant manifolds of stationary motions (IMSM), which correspond to integral  $V_2$ , can be written as

$$y_1 = p^2 - q^2 - x_0\gamma_1 = 0, \quad y_2 = 2p q - x_0\gamma_2 = 0. \quad (2)$$

It is Delaunay's manifold. The vector field on IMSM (2) is defined by the equations:

$$2\dot{p} = qr, \quad 2\dot{q} = -rp + x_0\gamma_3, \quad \dot{r} = -2pq, \quad \dot{\gamma}_3 = -q(p^2 + q^2)x_0^{-1}. \quad (3)$$

Differential equations (3) have the following first integrals:

$$2\tilde{H} = 4p^2 + r^2 = 2h, \quad \tilde{V}_1 = r\gamma_3 + 2p(p^2 + q^2)x_0^{-1} = m, \quad \tilde{V}_3 = \gamma_3^2 + (p^2 + q^2)^2x_0^{-2} = 1. \quad (4)$$

Let us state the problem of finding IMs of 2nd level on which the elements of algebra of the first integrals of system (3) assume a stationary value. To this end, we construct the following linear combination of integrals (4)

$$2\tilde{K} = 2\tilde{H} - 2\nu_1\tilde{V}_1 + \nu_1^2\tilde{V}_3. \quad (5)$$

The conditions of stationarity for  $\tilde{K}$  write

$$\begin{aligned} \frac{\partial \tilde{K}}{\partial p} &= 2\left(1 - \frac{\nu_1}{x_0}p\right)\left(2p - \frac{\nu_1}{x_0}(p^2 + q^2)\right) = 0, & \frac{\partial \tilde{K}}{\partial q} &= -\frac{2\nu_1q}{x_0}\left(2p - \frac{\nu_1}{x_0}(p^2 + q^2)\right) = 0, \\ \frac{\partial \tilde{K}}{\partial r} &= r - \nu_1\gamma_3 = 0, & \frac{\partial \tilde{K}}{\partial \gamma_3} &= -\nu_1(r - \nu_1\gamma_3) = 0. \end{aligned}$$

One of degenerated families of solutions of the above system is defined by the equations:

$$2\nu_1x_0p - \nu_1^2(p^2 + q^2) = 0, \quad r - \nu_1\gamma_3 = 0. \quad (6)$$

These are the equations of the family of IMSM on IMSM (2). The family of 2nd level IMSMs (6) can be "lifted up" as invariant into the initial phase space. To this end, it is necessary to add the Delaunay IMSM equations (2) to equations (6).

### 1.1 Kovalevskaya's Case. Enveloping Integral

In order to find peculiar IMSMs of 2nd level of system (3) let us apply enveloping integral for the family of integrals (5). Following to standard algorithm, we calculate derivative of integral  $\tilde{K}$  with respect to parameter  $\nu_1$  (the parameter of the family of integrals) and equate the obtained result to zero:

$$\frac{\partial \tilde{K}}{\partial \nu_1} = -\tilde{V}_1 + \nu_1\tilde{V}_3 = 0.$$

From the latter expression we find  $\nu_1 = \tilde{V}_1\tilde{V}_3^{-1}$ . Consequently, the enveloping first integral of our interest has the form:  $2\tilde{K}_0 = 2\tilde{K} - \tilde{V}_1^2\tilde{V}_3^{-1}$  or  $2\tilde{K}_0 = 2\tilde{H}\tilde{V}_3 - \tilde{V}_1^2$ .

Next, write down the necessary conditions of extremum for the integral  $\tilde{K}_0$ :

$$\begin{aligned} \frac{\partial \tilde{K}_0}{\partial p} &= 4p(\gamma_3^2 + (p^2 + q^2)x_0^{-2}) + 4p\left(2p^2 + \frac{r^2}{2}\right)(p^2 + q^2)x_0^{-2} - \\ &\quad 2(r\gamma_3 + 2px_0^{-1}(p^2 + q^2))(3p^2 + q^2)x_0^{-1} = 0, \\ \frac{\partial \tilde{K}_0}{\partial q} &= 4q(p^2 + q^2)x_0^{-2}\left(2p^2 + \frac{r^2}{2}\right) - 4pq(r\gamma_3 + 2px_0^{-1}(p^2 + q^2))x_0^{-1} = 0, \\ \frac{\partial \tilde{K}_0}{\partial r} &= r(\gamma_3^2 + (p^2 + q^2)x_0^{-2}) + (r\gamma_3 + 2px_0^{-1}(p^2 + q^2))\gamma_3 = 0, \\ \frac{\partial \tilde{K}_0}{\partial \gamma_3} &= 2\gamma_3\left(2p^2 + \frac{r^2}{2}\right) - (r\gamma_3 + 2px_0^{-1}(p^2 + q^2))r = 0. \end{aligned}$$

It can easily be verified that equation

$$(p^2 + q^2)r - 2px_0\gamma_3 = 0 \quad (7)$$

defines IMSM on which the enveloping integral assumes a stationary value, besides this IMSM is the first integral of equations (3). The 2nd level IMSM obtained by the above method can be "lifted up" into the phase space of the initial system. To this end, likewise above, we add the equation of Delaunay's IMSM to equation (7).

## 1.2 Kovalevskaya's Case. Stability.

Now let us consider the problem of stability for some above obtained IMSMs.

1. Let us write down the equations of perturbed motion in the neighborhood of Delaunay's IM (2):

$$\begin{aligned} \dot{y}_1 &= ry_2, \quad \dot{y}_2 = -ry_1, \quad 2\dot{p} = qr, \quad 2\dot{q} = -rp + x_0\gamma_3, \\ \dot{r} &= y_2 - 2pq, \quad x_0\dot{\gamma}_3 = -q(p^2 - q^2) + py_2 - qy_1. \end{aligned}$$

Here  $y_1 = p^2 - q^2 - x_0\gamma_1$ ,  $y_2 = 2pq - x_0\gamma_2$  are the deviations from Delaunay's IM in perturbed motion.

The system has the sign definite first integral

$$\Delta V_2 = y_1^2 + y_2^2 \gg 0.$$

The latter guaranties stability of IMSM (2).

2. Next, let us consider the family of IMSMs (6). Introduce the deviations from the elements of this family of IMSMs:

$$z_1 = 2x_0p - \nu_1(p^2 + q^2), \quad z_2 = r - \nu_1\gamma_3,$$

and write down differential equations of perturbed motion in this case. Because the first equation of IM is nonlinear, we use maps on the IMSMs. It is possible to take, for example, the following four maps when  $x_0\nu_1 > 0$ :

$$\begin{aligned} q &= \pm\sqrt{2px_0/\nu_1 - p^2}, \quad r = \nu_1\gamma_3, \quad (0 < p < 2x_0/\nu_1, -\nu_1 < r < \nu_1), \\ p &= x_0/\nu_1 \pm \sqrt{x_0^2/\nu_1^2 - q^2}, \quad r = \nu_1\gamma_3, \quad (-x_0/\nu_1 < q < x_0/\nu_1, -\nu_1 < r < \nu_1). \end{aligned}$$

Analogous maps can be constructed when  $x_0\nu_1 < 0$ . A vector field is defined in each map.

Let us write down equations of perturbed motion in the neighborhood of IM (6). In 4th map these equations have the form:

$$\begin{aligned} \dot{z}_1 &= x_0qz_2, \quad \dot{z}_2 = -qz_1/x_0, \quad \dot{r} = -2q(x_0/\nu_1 - \sqrt{x_0^2/\nu_1^2 - q^2 - z_1/\nu_1}), \\ 2\dot{q} &= -z_2x_0/\nu_1 + r\sqrt{x_0^2/\nu_1^2 - q^2 - z_1/\nu_1}. \end{aligned} \quad (8)$$

Analogous equations can also be written in other maps on IM (6). Equations (8) admit the first integral:

$$2\Delta K = z_2^2 + z_1^2/x_0^2.$$

In other maps the integral for equations of perturbed motion has analogous form. Because the integral is sign definite on  $z_1, z_2$ , we conclude that IMSM (6) is stable.

## 2 Kirchhoff's Problem

Let us consider the problem of motion of a rigid body in ideal fluid in case [5]. The differential equations of motion

$$\begin{aligned} \dot{r}_1 &= (\alpha r_1 + \beta r_2 + 2s_3)r_2 - r_3s_2, \quad \dot{r}_2 = -(\alpha r_1 + \beta r_2 + 2s_3)r_1 - r_3s_1, \quad \dot{r}_3 = r_1s_2 - r_2s_1, \\ \dot{s}_1 &= -(\beta s_3 + (\alpha^2 + \beta^2)r_2)r_3 + (\alpha r_1 + \beta r_2 + s_3)s_2, \\ \dot{s}_2 &= (\alpha s_3 + (\alpha^2 + \beta^2)r_1)r_3 - (\alpha r_1 + \beta r_2 + s_3)s_1, \quad \dot{s}_3 = (\beta r_1 - \alpha r_2)s_3 \end{aligned} \quad (9)$$

admit the following first integrals:

$$\begin{aligned} 2H &= (s_1^2 + s_2^2 + 2s_3^2) + 2(\alpha r_1 + \beta r_2)s_3 - (\alpha^2 + \beta^2)r_3^2 = 2h, \\ V_1 &= s_1r_1 + s_2r_2 + s_3r_3 = c_1, \quad 2V_2 = r_1^2 + r_2^2 + r_3^2 = c_2, \\ 2V_3 &= (r_1s_1 + r_2s_2)((\alpha^2 + \beta^2)(r_1s_1 + r_2s_2) + 2(\alpha s_1 + \beta s_2)s_3) \\ &\quad + s_3^2(s_1^2 + s_2^2 + (\alpha r_1 + \beta r_2 + s_3)^2) = 2c_3. \end{aligned} \quad (10)$$

In order to find stationary solutions and IMSMs of system (9) we construct the families  $K$  of first integrals

$$K = \lambda_0 H - \lambda_1 V_1 - \lambda_2 V_2 - \lambda_3 V_3. \quad (11)$$

from problem's first integrals (10).

The necessary conditions of extremum for  $K$  (11) with respect to variables  $s_1, s_2, s_3, r_1, r_2, r_3$

$$\begin{aligned}
\frac{\partial K}{\partial s_1} &= \lambda_0 s_1 - \lambda_1 r_1 - \lambda_3 [(\alpha^2 + \beta^2) r_1 (r_1 s_1 + r_2 s_2) + s_2 s_3 (\alpha r_2 + \beta r_1) + s_1 s_3 (2\alpha r_1 + s_3)] = 0, \\
\frac{\partial K}{\partial s_2} &= \lambda_0 s_2 - \lambda_1 r_2 - \lambda_3 [(\alpha^2 + \beta^2) r_2 (r_1 s_1 + r_2 s_2) + s_1 s_3 (\alpha r_2 + \beta r_1) + s_2 s_3 (2\beta r_2 + s_3)] = 0, \\
\frac{\partial K}{\partial s_3} &= \lambda_0 (\alpha r_1 + \beta r_2 + 2s_3) - \lambda_1 r_3 - \lambda_3 [(\alpha s_1 + \beta s_2) (r_1 s_1 + r_2 s_2) + \\
&\quad s_3 ((\alpha r_1 + \beta r_2 + 2s_3)^2 + s_1^2 + s_2^2 - s_3 (\alpha r_1 + \beta r_2 + 2s_3))] = 0, \\
\frac{\partial K}{\partial r_1} &= \lambda_0 \alpha s_3 - \lambda_1 s_1 - \lambda_2 r_1 - \lambda_3 [(\alpha^2 + \beta^2) s_1 (r_1 s_1 + r_2 s_2) + s_1 s_3 (\alpha s_1 + \beta s_2) \\
&\quad + \alpha s_3^2 (\alpha r_1 + \beta r_2) + \alpha s_3^3] = 0, \\
\frac{\partial K}{\partial r_2} &= \beta \lambda_0 s_3 - \lambda_1 s_2 - \lambda_2 r_2 - \lambda_3 [(\alpha^2 + \beta^2) (r_1 s_1 + r_2) s_2 + (\alpha s_1 + \beta s_2) s_2 s_3 \\
&\quad + \beta s_3^2 (\alpha r_1 + \beta r_2) + \beta s_3^3] = 0, \\
\frac{\partial K}{\partial r_3} &= -((\alpha^2 + \beta^2) \lambda_0 + \lambda_2) r_3 - \lambda_1 s_3 = 0. \tag{12}
\end{aligned}$$

define the families of stationary solutions and the families of IMSM of differential equations (9). Computer algebra system MATHEMATICA allows one to apply the Gröbner basis technique [6] for finding solutions of nonlinear algebraic system. The Gröbner basis for system (12) constructed with respect to some part of parameters  $\lambda_0, \lambda_1, \lambda_2$  and some part of phase variables  $r_3, s_3$  writes:

$$\begin{aligned}
&\{ \lambda_2 (pz^2 \lambda_2 + q^2 x^2 \lambda_3), -q^2 x \lambda_1 - z ((\beta r_1 + \alpha r_2) s_1^2 + 2(-\alpha r_1 + \beta r_2) s_1 s_2 - (\beta r_1 + \alpha r_2) s_2^2) \\
&\lambda_2 - Gq^2 x^2 \lambda_3, -pq^2 \lambda_0 - (\beta^2 r_1^4 - 2\alpha \beta r_1^3 r_2 + r_2^2 (\alpha^2 r_2^2 + s_1^2)) - 2r_1 (\alpha \beta r_2^3 + r_2 s_1 s_2) + \\
&r_1^2 (Gr_2^2 + s_2^2) \lambda_2, -yz \lambda_2 - q^2 x s_3 \lambda_3, -pz (\alpha r_1 + \beta r_2) \lambda_2 + qx^2 (Gr_3 - \alpha s_1 - \beta s_2) \lambda_3 \}. \tag{13}
\end{aligned}$$

Here the following denotations

$$q = \beta s_1 - \alpha s_2, \quad x = r_1 s_1 + r_2 s_2, \quad y = r_1 s_2 - r_2 s_1, \quad z = \beta r_1 - \alpha r_2, \quad G = \alpha^2 + \beta^2, \quad p = r_1^2 + r_2^2. \tag{14}$$

were used.

Let us consider one family of solutions of system (13) (here  $\lambda_3$  is the family parameter):

$$\begin{aligned}
s_3 &= xy/pz, \quad r_3 = y/z, \quad \lambda_2 = -q^2 x^2 \lambda_3 / pz^2, \\
\lambda_1 &= - (x (-pq^2 + Gy^2 + Gpz^2) \lambda_3) / pz^2, \quad \lambda_0 = x^2 (y^2 + pz^2) \lambda_3 / pz^2. \tag{15}
\end{aligned}$$

Analysis of the above relations showed that expressions for  $r_3, s_3$  (15) define IMSM of differential equations (9). The vector field on IMSM (15) is described by equations

$$\begin{aligned}
\dot{r}_1 &= r_2 \left( \frac{2xy}{pz} + \alpha r_1 + \beta r_2 \right) - \frac{ys_2}{z}, \quad \dot{r}_2 = -r_1 \left( \frac{2xy}{pz} + \alpha r_1 + \beta r_2 \right) + \frac{ys_1}{z}, \\
\dot{s}_1 &= \frac{-y(xy\beta + Gpzr_2) + z(xy + pz(\alpha r_1 + \beta r_2)) s_2}{pz^2}, \\
\dot{s}_2 &= \frac{y(xy\alpha + Gpzr_1) - z(xy + pz(\alpha r_1 + \beta r_2)) s_1}{pz^2}. \tag{16}
\end{aligned}$$

The expressions  $\lambda_0, \lambda_1, \lambda_2$  (15) are the first integrals of equations (16). It can be showed that these integrals correspond to the integrals of initial differential equations (9):

$$\begin{aligned}
\tilde{\lambda}_0 &= (V_1(HV_1 \pm \sqrt{(v_1^2(H^2 - 2V_3) + 8GV_2^2 V_3) \lambda_3}) / (V_1^2 - 4GV_2^2)), \\
\tilde{\lambda}_1 &= ((2GHV_1 V_2^2 \pm (V_1^2 - 2GV_2^2) \sqrt{(H^2 v_1^2 - 2V_1^2 V_3 + 8GV_2^2 V_3) \lambda_3}) / (V_2(V_1^2 - 4GV_2^2))), \\
\tilde{\lambda}_2 &= (V_1^2(4GHV_2^2 \pm V_1 \sqrt{(v_1^2(H^2 - 2V_3) + 8GV_2^2 V_3) \lambda_3}) / (V_1^2 - 4GV_2^2)).
\end{aligned}$$

## 2.1 Second Level Invariant Manifolds

Let us find IMSMs of 2nd level on IM (15). For this purpose, we shall use narrowing of the integral  $K$  on IMSM (15). First integrals (10) on IM (15) in denotations (14) have the form:

$$\begin{aligned}\tilde{H} &= vx - \frac{q^2x}{2vz^2} + \frac{v^2y^2}{z^2}, \quad \tilde{V}_1 = x + \frac{vy^2}{z^2}, \quad \tilde{V}_2 = \frac{vy^2 + xz^2}{2vz^2}, \\ \tilde{V}_3 &= \frac{(vy^2 + xz^2)(-q^2x + (G + v^2)(vy^2 + xz^2))}{2z^4},\end{aligned}$$

Using above integrals and taking into account expressions for  $\lambda_0, \lambda_1, \lambda_2$  (15), we can write integral  $K$  (11) on IMSM (15) as:

$$\tilde{K} = v^2W_{12}(W_{21} + 2GW_{12} + 2v^2W_{12})\lambda_3 = v^2W_{12}Q, \quad (17)$$

where  $v = x/p$ ,  $W_{12} = (y^2 + pz^2)/2z^2$ ,  $W_{21} = -pq^2/z^2$  are the first integrals of differential equations (16) on IMSM (15). The conditions of stationarity for  $\tilde{K}$  (17) enable us to immediately obtain one of stationary solutions of the problem. It has the form

$$v = x/p = (r_1s_1 + r_2s_2)/(r_1^2 + r_2^2) = 0. \quad (18)$$

The rest solutions are determined by equations:

$$2\frac{\partial v}{\partial x_i}W_{12}Q + v\left(\frac{\partial W_{12}}{\partial x_i}Q + W_{12}\frac{\partial Q}{\partial x_i}\right) = 0, \quad (i = \overline{1,4}) \quad (19)$$

where  $x_1 = r_1$ ,  $x_2 = r_2$ ,  $x_3 = s_1$ ,  $x_4 = s_2$ .

We shall not analyze system (19) here, only note that 2nd level IMSM (18) is stable, because  $v$  is the first integral of equations (16). We also note that equation (18) defines IM of initial differential equations.

All calculations have been performed with the aid of Mathematica system and program package [7] written in Mathematica language.

The work was supported by the Program of Fundamental Researches of Presidium of the Russian Academy of Sciences no. 17.1.

## References

- [1] *Lyapunov A.M.* The constant helical motions of a rigid body an fluid. Collected Papers. Moscow: izd. Akad. Nauk SSSR, 1954, 1, pp. 276-319
- [2] *Irtegov V.D.* On specificities of families of invariant manifolds of conservative systems. *Izvestiya VUZov Matematika*, 2010. no.8, pp. 42-50
- [3] *Irtegov v.D., Titorenko T.N.* The invariant manifolds of systems with first integrals // *J. of Applied Mathematics and Mechanics*, 73, 2009, pp.379-384
- [4] *Kovalevski S.* Sur le probleme de la rotation d'un corps solide autor d'un point fixe. // *Acta Math.* 1888, V.12, pp.177-232
- [5] *Sokolov, V.V.* A new integrable case for the Kirchhoff equations. *Theoret. and Math. Phys.* 1(129), 2001, pp.1335-1340
- [6] *Cox D., Little J., O'Shea D.*, Ideals, Varieties and Algorithms, N.Y, Springer, 1997, 513 p.
- [7] *Banshchikov, A.V., Burlakova L.A., Irtegov V.D., Titorenko T.N.* The software package for selecting and investigation the stability of stationary sets of mechanical systems. Certificate of state registration of the program on a computer, number 2011615235, on July 5, 2011 (in Russian)

# Orbital Reversibility of Planar Dynamical Systems

Antonio Algaba, Isabel Checa, Cristóbal García  
University of Huelva (Spain)

Estanislao Gamero  
University of Sevilla (Spain)

isabel.checa@dmat.uhu.es

## Abstract

We give a necessary condition for the orbital-reversibility of a planar system, namely, the existence of a normal form under equivalence which is reversible to the change of sign in the first variable. Based in this condition, we formulate a suitable algorithm to detect orbital-reversibility and we apply the results to solve the center problem in a family of planar nilpotent systems.

## Keywords

Bifurcation, Reversible system, Center problem, Orbital Reversible system

## 1 Introduction

Consider a planar autonomous system of differential equations having an equilibrium point at the origin given by

$$\dot{\mathbf{x}} = \mathbf{F}(\mathbf{x}), \quad (1.1)$$

where  $\mathbf{x} = (x, y)^T \in \mathbb{R}^2$ . We study if it admits some reversibility modulo  $\mathcal{C}^\infty$ -equivalence (see [1] and [2]).

The problem of determining if system (1.1) has some reversibility is consider in [3] and [4]. In this work, we study if there exists some time-reparametrization such that the resulting system admits some reversibility. The existence of some orbital-reversibility is a valuable feature that helps in the understanding of the dynamical behaviour of a given system.

Next, we give a precise definition of the reversibility we will deal with:

An involution is a local diffeomorphism  $\sigma \in \mathcal{C}^\infty$ , such that  $\sigma \circ \sigma = Id$ ,  $\sigma(\mathbf{0}) = \mathbf{0}$  and  $\text{codim}(\text{Fix}(\sigma)) = 1$ , where  $\text{Fix}(\sigma) = \{\mathbf{x} \in \mathbb{R}^n : \sigma(\mathbf{x}) = \mathbf{x}\}$  is the fixed point set of  $\sigma$ .

We say that system (1.1) is reversible if there exists some involution  $\sigma$  such that  $\sigma_* \mathbf{F} = -\mathbf{F}$ .

We say that system (1.1) is orbital-reversible if there exist an involution  $\sigma$  and a function  $\mu \in \mathcal{C}^\infty$ , with  $\mu(\mathbf{0}) = 1$  such that  $\sigma_* (\mu \mathbf{F}) = -\mu \mathbf{F}$ , (this means that  $\mathbf{F}$  is reversible modulo a time-reparametrization).

We have denoted the pull-back of a vector field of  $\mathbf{F}$  by a transformation  $\Phi$  as  $\Phi_* \mathbf{F}$ . If we use a generator of the transformation, the notation  $\mathbf{U} ** \mathbf{F} := \Phi_* \mathbf{F}$  will be used instead. The transformed system can be expressed in terms of nested Lie products. Let us define  $T_{\mathbf{U}}^{(0)}(\mathbf{F}) := \mathbf{F}$ , and

$$T_{\mathbf{U}}^{(l)}(\mathbf{F}) := T_{\mathbf{U}}^{(l-1)}([\mathbf{F}, \mathbf{U}]) = \overbrace{[\dots[\mathbf{F}, \mathbf{U}], \dots, \mathbf{U}]}^{l \text{ times}} = [T_{\mathbf{U}}^{(l-1)}(\mathbf{F}), \mathbf{U}], \quad \text{for } l \geq 1.$$

If we use both, a nonlinear time-reparametrization  $dt = \mu(\mathbf{x})dT$  and a near-identity transformation with generator  $\mathbf{U}(\mathbf{x})$ , then the transformed vector field is given by:

$$\mathbf{U} ** ((1 + \mu)\mathbf{F}) = \mathbf{U} ** \mathbf{F} + \mu \mathbf{F} + \mu [\mathbf{F}, \mathbf{U}] + (\nabla \mu \cdot \mathbf{U})\mathbf{F} + \frac{1}{2!} [[\mu \mathbf{F}, \mathbf{U}], \mathbf{U}] + \dots \quad (1.2)$$

In our study, we assume a quasi-homogeneous expansion for the vector field  $\mathbf{F}$  corresponding to a type  $\mathbf{t} = (t_1, t_2) \in \mathbb{N}^2$ . So, we can suppose that  $\mathbf{F}$  is of the form

$$\mathbf{F}(\mathbf{x}) = \tilde{\mathbf{F}}_r(\mathbf{x}) + \mathbf{F}_{r+1}(\mathbf{x}) + \dots, \quad \text{for some } r \in \mathbb{Z}, \quad (1.3)$$

where the lowest-degree quasi-homogeneous term  $\tilde{\mathbf{F}}_r \neq \mathbf{0}$  is  $R_x$ -reversible, and  $\mathbf{F}_{r+k} \in \mathcal{Q}_{r+k}^t$  for all  $k \in \mathbb{N}$ .

## 2 Some Definitions and Main Result

In this section, we introduce some definitions and we present our important result.

Firstly, we introduce the following vector spaces:

- $\mathcal{O}_k^t = \{\mu \in \mathcal{P}_k^t : \mu(-x, y) = -\mu(x, y)\}$ , the set of quasi-homogeneous scalar functions of degree  $k$  which are odd in the first variable.
- $\mathcal{E}_k^t = \{\mu \in \mathcal{P}_k^t : \mu(-x, y) = \mu(x, y)\}$ , the set of quasi-homogeneous scalar functions of degree  $k$  which are even in the first variable.
- $\mathcal{R}_k^t = \{\mathbf{F} = (P, Q)^T \in \mathcal{Q}_k^t : P \in \mathcal{E}_{k+t_1}^t, Q \in \mathcal{O}_{k+t_2}^t\}$ , the set of  $R_x$ -reversible quasi-homogeneous vector fields of degree  $k$ .
- $\mathcal{S}_k^t := \{\mathbf{F} = (P, Q)^T \in \mathcal{Q}_k^t : P \in \mathcal{O}_{k+t_1}^t, Q \in \mathcal{E}_{k+t_2}^t\}$ , the set of  $R_x$ -symmetric quasi-homogeneous vector fields of degree  $k$ .

It is easy to deduce that  $\mathcal{P}_k^t = \mathcal{O}_k^t \oplus \mathcal{E}_k^t$  and  $\mathcal{Q}_k^t = \mathcal{R}_k^t \oplus \mathcal{S}_k^t$ . This decomposition allow us to define the corresponding projection operators as follows:

$$\begin{aligned} \pi^{(\circ)}(\mu) &\in \bigoplus_k \mathcal{O}_k^t, & \pi^{(\text{e})}(\mu) &\in \bigoplus_k \mathcal{E}_k^t, & \text{for } \mu &\in \bigoplus_k \mathcal{P}_k^t, \text{ and} \\ \Pi^{(\text{r})}(\mathbf{U}) &\in \bigoplus_k \mathcal{R}_k^t, & \Pi^{(\text{s})}(\mathbf{U}) &\in \bigoplus_k \mathcal{S}_k^t, & \text{for } \mathbf{U} &\in \bigoplus_k \mathcal{Q}_k^t. \end{aligned}$$

The main goal of this paper is to determine conditions for the orbital-reversibility of (1.3), which will be based on the existence of a near-identity transformation  $\Phi = \sum_{j \geq 0} \Phi_j$ , ( $\Phi_j \in \mathcal{Q}_j^t$ ), and a scalar function  $\mu \in \mathcal{C}^\infty$ , with  $\mu(\mathbf{0}) = 1$ , such that  $\Phi_* (\mu \mathbf{F})$  is  $R_x$ -reversible.

For our convenience, from now on we will write the time-reparametrization as  $1 + \mu$ , with  $\mu(\mathbf{0}) = 0$ . Indeed, it will be written as  $1 + \sum_{j \geq 1} \mu_j$ , where  $\mu_j \in \mathcal{P}_j^t$  for  $j \geq 1$ .

**Definition 1** *We say that the vector field of system (1.3) is  $N$ -orbital-reversible ( $N \in \mathbb{N}$ ) if there exist a vector field  $\mathbf{U} \in \bigoplus_{j \geq 1} \mathcal{Q}_j^t$  and a scalar function  $\mu \in \bigoplus_{j \geq 1} \mathcal{P}_j^t$ , such that  $\mathcal{J}^{r+N}(\mathbf{U} ** ((1 + \mu)\mathbf{F}))$  is  $R_x$ -reversible.*

Our idea is to adapt the normal form procedure in order to determine conditions under which the normalized vector field is  $N$ -orbital-reversible. We introduce the Lie derivate along the lowest-degree quasi-homogeneous term  $\tilde{\mathbf{F}}_r$ :

$$\begin{aligned} \ell_{k-r} &: \mathcal{P}_{k-r}^t \longrightarrow \mathcal{P}_k^t \\ &\mu_{k-r} \longrightarrow \nabla \mu_{k-r} \cdot \tilde{\mathbf{F}}_r. \end{aligned}$$

In the normal form reduction it is enough to take its quasi-homogeneous terms  $\mu_k$  belonging to  $\text{Cor}(\ell_{k-r})$  (a complementary subspace to  $\text{Range}(\ell_{k-r})$ ).

We denote

$$\hat{\mathcal{R}}_k^t := \mathcal{R}_k^t \cap \hat{\mathcal{Q}}_k^t \quad \text{and} \quad \hat{\mathcal{O}}_k^t := \mathcal{O}_k^t \cap \text{Cor}(\ell_{k-r}),$$

where  $\hat{\mathcal{Q}}_k^t$  is a complementary subspace to  $\text{Ker}(\ell_{k-r})\tilde{\mathbf{F}}_r$  in  $\mathcal{Q}_k^t$ .

Next, we plain to deduce some facts about the normal forms for orbital-reversible vector fields. To this end, we use that  $\mathcal{Q}_k^t = \mathcal{R}_k^t \oplus \mathcal{S}_k^t$ , which allows to write the vector field (1.3) as:

$$\mathbf{F} = \tilde{\mathbf{F}}_r + \sum_{j=1}^{\infty} (\tilde{\mathbf{F}}_{r+j} + \bar{\mathbf{F}}_{r+j}), \quad (2.4)$$

where  $\tilde{\mathbf{F}}_{r+j} = \Pi^{(\text{r})}(\mathbf{F}_{r+j}) \in \mathcal{R}_{r+j}^t$  and  $\bar{\mathbf{F}}_{r+j} = \Pi^{(\text{s})}(\mathbf{F}_{r+j}) \in \mathcal{S}_{r+j}^t$ .

To describe a normal form procedure well adapted to the orbital-reversibility problem, let us denote the above vector field as

$$\mathbf{F}^{(0)} := \mathbf{F} = \tilde{\mathbf{F}}_r^{(0)} + (\tilde{\mathbf{F}}_{r+1}^{(0)} + \bar{\mathbf{F}}_{r+1}^{(0)}) + \dots$$



We observe that the lowest-degree quasi-homogeneous term is reversible:  $\tilde{\mathbf{F}}_r^{(0)} \in \mathcal{R}_r^{\mathbf{t}}$ .

We define the homological operator  $\bar{\mathcal{L}}^{(m)}$  as,

$$\begin{aligned} \bar{\mathcal{L}}^{(1)} : \widehat{\mathcal{R}}_1^{\mathbf{t}} \times \widehat{\mathcal{O}}_1^{\mathbf{t}} &\longrightarrow \mathcal{S}_{r+1}^{\mathbf{t}} \\ (\tilde{\mathbf{U}}_1, \tilde{\mu}_1) &\longrightarrow -[\tilde{\mathbf{F}}_r^{(0)}, \tilde{\mathbf{U}}_1] - \tilde{\mu}_1 \tilde{\mathbf{F}}_r^{(0)}, \end{aligned}$$

and

$$\begin{aligned} \bar{\mathcal{L}}^{(m)} : \text{Ker}(\bar{\mathcal{L}}^{(m-1)}) \times (\widehat{\mathcal{R}}_m^{\mathbf{t}}, \widehat{\mathcal{O}}_m^{\mathbf{t}}) &\longrightarrow \mathcal{S}_{r+m}^{\mathbf{t}} \\ (\tilde{\mathbf{U}}_1, \tilde{\mu}_1, \dots, \tilde{\mathbf{U}}_{m-1}, \tilde{\mu}_{m-1}; \tilde{\mathbf{U}}_m, \tilde{\mu}_m) &\longrightarrow -\sum_{j=0}^{m-1} [\tilde{\mathbf{F}}_{r+j}^{(m-1)}, \tilde{\mathbf{U}}_{m-j}] - \tilde{\mu}_{m-j} \tilde{\mathbf{F}}_{r+j}^{(m-1)}. \end{aligned}$$

It is evident that operator  $\bar{\mathcal{L}}^{(m)}$  depends on  $\tilde{\mathbf{F}}_r^{(m)}, \dots, \tilde{\mathbf{F}}_{r+m-1}^{(m)}$ .

The following result characterizes the  $(N+1)$ -orbital-reversibility of a vector field  $N$ -orbital-reversible. Proceeding degree by degree and following the ideas of the classical normal form theory, we obtain an algorithm to discarding cases the orbital-reversibility based of the next theorem.

**Theorem 2** *Let us consider a vector field  $\mathbf{F} = \tilde{\mathbf{F}}_r + \dots + \tilde{\mathbf{F}}_{r+N-1} + (\tilde{\mathbf{F}}_{r+N} + \bar{\mathbf{F}}_{r+N}) + \dots$ , satisfying  $\bar{\mathbf{F}}_{r+N} \neq 0$  and  $\text{Proj}_{\text{Im}(\bar{\mathcal{L}}^{(N)})}(\bar{\mathbf{F}}_{r+N}) = \mathbf{0}$ , for some  $N \in \mathbb{N}$ . Then,  $\mathbf{F}$  is not orbital-reversible.*

### 3 Application

Let us consider the following family of planar vector fields:

$$\begin{pmatrix} \dot{x} \\ \dot{y} \end{pmatrix} = \begin{pmatrix} y \\ \sigma x^{4q+1} \end{pmatrix} + \begin{pmatrix} a_1 xy + a_2 x^{2q+2} \\ b_1 y^2 + b_2 x^{2q+1} y \end{pmatrix}, \quad (3.5)$$

where  $\sigma = \pm 1$ ,  $q \in \mathbb{N}$ .

This family has been studied by several authors. Namely, the analytic integrability for this family has been studied in [5]; the center problem for  $\sigma = -1$  (which corresponds to the monodromic situation) has been partially studied in [6]; and the reversibility problem is completely solved in [3]. With respect to the orbital-reversibility problem, we have the following result:

**Theorem 3** *System (3.5) is orbital-reversible if and only if one of the following conditions is satisfied:*

- (a)  $a_2 = b_2 = 0$ .
- (b)  $a_2 = a_1 = b_1 = 0$ ,  $b_2 \neq 0$ .
- (c)  $a_1 = b_1 = 0$ ,  $a_2 \neq 0$ .
- (d)  $a_1 + 2b_1 = b_2 + 2(q+1)a_2 = 0$ ,  $a_2 b_1 \neq 0$ .
- (e)  $b_2 = (2q+1)a_2$ ,  $b_1 = (2q+1)a_1$ ,  $a_2(a_1 + 2b_1) \neq 0$ .

Proof:

The vector field of the statement can be written as  $\mathbf{F} = \tilde{\mathbf{F}}_r + \mathbf{F}_{r+1}$ , where

$$\tilde{\mathbf{F}}_r := (y, \sigma x^{4q+1})^T \in \mathcal{Q}_{2q}^{\mathbf{t}}, \text{ and } \mathbf{F}_{r+1} \in \mathcal{Q}_{2q+1}^{\mathbf{t}},$$

being  $r = 2q$  and  $\mathbf{t} = (1, 2q+1)$ . We observe that  $\tilde{\mathbf{F}}_{2q}$  is  $R_x$ - and  $R_y$ -reversible. It is enough to study the  $R_x$ - and the  $R_y$ -orbital-reversibility of the vector field  $\mathbf{F}$ .

( $\star$ ) We start with the  $R_x$ -orbital-reversibility. As we will see later, in this case is sufficient to reach the  $N = 8$ -orbital-reversibility to solve the orbital-reversibility problem. To reduce the vector field of the statement to the normal form  $\mathbf{F}^{(8)}$ , we take the generator

$$\tilde{\mathbf{U}} = \begin{pmatrix} \alpha_1 x^2 \\ \alpha_2 xy \end{pmatrix} + \begin{pmatrix} 0 \\ \alpha_3 x^{2q+3} \end{pmatrix} + \begin{pmatrix} \alpha_4 x^4 \\ \alpha_5 x^3 y \end{pmatrix} + \dots \in \bigoplus_{j=1}^8 \mathcal{R}_j^{\mathbf{t}},$$

and the time-reparametrization associated to

$$\tilde{\mu} = \gamma_1 x + \gamma_3 x^3 + \gamma_5 x^5 + \gamma_7 x^7 \in \bigoplus_{j \geq 1}^8 \widehat{\mathcal{O}}_j^t,$$

where  $\alpha_i$  and  $\gamma_i$  are arbitrary parameters. Using *Maple* in the computations, we obtain the following normal form:

$$\begin{aligned} \mathbf{F}^{(8)} &= \tilde{\mathbf{U}}_{**}((1 + \tilde{\mu})\mathbf{F}) = \tilde{\mathbf{F}}_{2q} + \tilde{\mathbf{F}}_{2q+1} + (\tilde{\mathbf{F}}_{2q+2} - \frac{1}{3(4q+3)}\lambda^{(2)} \begin{pmatrix} 0 \\ x^{2q+2}y \end{pmatrix}) \\ &+ \tilde{\mathbf{F}}_{2q+3} + (\tilde{\mathbf{F}}_{2q+4} + \frac{\sigma}{3(4q+5)(4q+3)^3}\lambda^{(4)} \begin{pmatrix} 0 \\ x^{2q+4}y \end{pmatrix}) \\ &+ \tilde{\mathbf{F}}_{2q+5} + (\tilde{\mathbf{F}}_{2q+6} + \lambda^{(6)} \begin{pmatrix} 0 \\ x^{2q+6}y \end{pmatrix}) \\ &+ \tilde{\mathbf{F}}_{2q+7} + (\tilde{\mathbf{F}}_{2q+8} + \lambda^{(8)} \begin{pmatrix} 0 \\ x^{2q+8}y \end{pmatrix}) + \dots \end{aligned}$$

So, by applying Theorem 2, if  $\mathbf{F}$  is orbital-reversible then the coefficients  $\lambda^{(2j)}$  must vanish.

The first normal form coefficient  $\lambda^{(2j)}$  is:

$$\lambda^{(2)} = a_2((2q+3)(2q+1)a_1 + 2qb_1) + b_2(2qa_1 - 3b_1). \quad (3.6)$$

To study the vanishing of this coefficient, we consider the following two possibilities:

(1)  $2qa_1 - 3b_1 = 0$ , and then  $\lambda^{(2)}$  vanishes in a couple of cases:

(1a)  $a_2 = 0$ . In this case, the next normal form coefficient is

$$\lambda^{(4)} = qb_2a_1^3,$$

which vanishes if  $b_2 = 0$  (in this case, covered in item (a), the system is  $R_y$ -reversible), or if  $a_1 = 0$  (now, the system is  $R_x$ -reversible; this situation is described in item (b)).

(1b)  $a_2 \neq 0$ ,  $(2q+3)(2q+1)a_1 + 2qb_1 = 0$ , which provides  $a_1 = b_1 = 0$ . In this case the system is  $R_x$ -reversible. This is the situation described in item (c).

(2)  $2qa_1 - 3b_1 \neq 0$ , and then  $\lambda^{(2)}$  vanishes if, and only if,

$$b_2 = -\frac{(2q+3)(2q+1)a_1 + 2qb_1}{2qa_1 - 3b_1}a_2. \quad (3.7)$$

For this value, the next normal form coefficient is

$$\lambda^{(4)} = \frac{4q+3}{2qa_1 - 3b_1}a_2(a_1 + 2b_1)(b_1 - (2q+1)a_1)p_4(a_2, a_1, b_1, q, \sigma),$$

where we have denoted

$$\begin{aligned} p_4(a_2, a_1, b_1, q, \sigma) &= 3(2q+5)(4q+3)^2((2q+3)(4q+1)a_1 - (4q+9)b_1)a_2^2 \\ &+ \sigma(2qa_1 - 3b_1)(2q(120q^2 + 202q + 49)a_1^2 - (512q^2 + 844q + 135)a_1b_1 + 5(52q + 81)b_1^2). \end{aligned}$$

The vanishing of  $\lambda^{(4)}$  leads to some subcases:

(2a)  $a_2 = 0$ , which implies  $b_2 = 0$ . We get again item (a).

(2b)  $a_2 \neq 0$ ,  $a_1 + 2b_1 = 0$ . This hypothesis implies that  $b_1 \neq 0$  (otherwise,  $a_1 = b_1 = 0$ ). Moreover, the equation (3.7) reduces to  $b_2 = -2(q+1)a_2$ . Now, the system (3.5) is Hamiltonian, with Hamiltonian

$$h(x, y) = -\frac{1}{2}y^2 + \frac{\sigma}{2(2q+1)}x^{4q+2} + b_1xy^2 - a_2x^{2q+2}y.$$

If we denote  $u = x$ ,  $v = y - 2b_1xy + a_2x^{2q+2}$ , then system (3.5) becomes:

$$\begin{aligned} \dot{u} &= v, \\ \dot{v} &= \sigma u^{4q+4} + (2(q+1)a_2^2 - 2b_1\sigma)u^{4q+2} + \frac{a_2u^{4q+4} - b_1v^2}{1 - 2b_1u}, \end{aligned}$$

which is  $R_v$ -reversible (item (d)).

(2c)  $a_2(a_1 + 2b_1) \neq 0$ ,  $b_1 = (2q + 1)a_1$ . Now, the equation (3.7) reduces to  $b_2 = (2q + 1)a_2$ .

In this case, it is more convenient to work with system (3.5) with the transformation  $x = u$ ,  $y = v(1 + a_1u)^{2q+1}$ , i.e.:

$$\begin{aligned}\dot{u} &= v(1 + a_1u)^{2q+2} + a_2u^{2q+2}, \\ \dot{v} &= \frac{\sigma u^{4q+1}}{(1 + a_1u)^{2q+1}} + \frac{(2q + 1)a_2}{1 + a_1u}u^{2q+1}v.\end{aligned}$$

The time reparametrization  $dT = (1 + a_1X)^{2q}dt$  and the transformation  $X = \frac{u}{1+a_1u}$ ,  $Y = v$ , yield

$$\begin{aligned}X' &= Y + a_2X^{2q+2}, \\ Y' &= \sigma X^{4q+1} + (2q + 1)a_2X^{2q+1}Y,\end{aligned}$$

which is  $R_X$ -reversible (item (e)).

(2d)  $a_2(a_1 + 2b_1)(b_1 - (2q + 1)a_1) \neq 0$ ,  $p_4(a_2, a_1, b_1, q, \sigma) = 0$ . In this case, both coefficients  $\lambda^{(6)}$  and  $\lambda^{(8)}$  can not vanish simultaneously, and the vector field is not orbital-reversible.

( $\star\star$ ) The situation with the  $R_y$ -orbital-reversibility does not include any new case.

From the proof of the theorem, we obtain that system (3.5) is orbital-reversible if, and only if, it is 8-orbital reversible.

## References

- [1] J.S.W. Lamb and J.A.G. Roberts. *Time-reversal symmetry in dynamical systems: a survey*. Physica D. Nonlinear Phenomena, 112, 1-2, (1998), pp. 1-39.
- [2] D. Montgomery and L. Zippin. *Topological Transformations Group*. Interscience Publ., New York, 1995.
- [3] A. Algaba, C. García and M.A. Teixeira. *Reversibility and quasi-homogeneous normal forms of vector fields*. Nonlinear Analysis: Theory, Methods and Applications, 73, (2010), pp. 510-525.
- [4] A. Algaba, E. Gamero and C. García. *The reversibility problem for quasi-homogeneous dynamical systems*. Discrete and Continuous Dynamical System-A, 33, 8, (2013), pp. 3225-3236. doi:10.3934/dcds.2013.33.3225
- [5] J. Chavarriga, I. García and J. Giné. *Integrability of centers perturbed by quasi-homogeneous polynomials*. Journal of Mathematical Analysis and Applications, 210 (1997), pp. 268-278.
- [6] A. Gasull and J. Torregrosa. *Center problem for several differential equations via Cherkas' method*. Journal of Mathematical Analysis and Applications, 228 (1998), pp. 322-343.

# The Study of Isochronicity and Critical Period Bifurcations on Center Manifolds of 3-dim Polynomial Systems Using Computer Algebra

Matej Mencinger<sup>1,2</sup>, Brigita Ferčec<sup>3</sup>

<sup>1</sup>FCE, University of Maribor (Slovenia)

<sup>2</sup>IMFM, Ljubljana (Slovenia)

<sup>3</sup>CAMTP, University of Maribor (Slovenia)

matej.mencinger@um.si

## Abstract

Using the solution of the center-focus problem from [4], we present the investigation of isochronicity and critical period bifurcations of two families of cubic 3-dim systems of ODEs. Both cubic systems have a center manifold filled with closed trajectories. The presented study is performed using computer algebra systems MATHEMATICA and SINGULAR.

## Keywords

Polynomial systems of ODEs, center manifolds, isochronicity, bifurcation of critical periods, CAS

## 1 Introduction

The main topic of our work is the investigation of the quadratic 3D system of ODEs

$$\begin{aligned}\dot{u} &= -v + au^2 + av^2 + cuw + dvw, \\ \dot{v} &= u + bu^2 + bv^2 + euw + fvw, \\ \dot{w} &= -w + Su^2 + Sv^2 + Tuw + Uvw,\end{aligned}\tag{1}$$

with real coefficients  $a, b, c, d, e, f, S, T$  and  $U$ . System (1) was studied already in [4], and further in [5], [8], where planar polynomial systems of ODEs appearing on the center manifold of (1) were investigated.

We present the criteria on the coefficients of the system to distinguish between the cases of isochronous and non-isochronous oscillations, considered in [5] and [8]. Bifurcations of critical periods of the system are studied as well. Both phenomena as well as the linearization and the derivation of the period function (2) and the linearizability quantities are defined in the following section.

In order to study the period function

$$T(r) = 2\pi \left( 1 + \sum_{k=1}^{\infty} T_k r^k \right)\tag{2}$$

of the centers on the center manifolds and obtain the necessary and sufficient conditions of isochronicity of the centers and to describe the critical period bifurcations (c.f. [10]) we have used the computer algebra system MATHEMATICA and the special purpose computer algebra system SINGULAR [7], which has powerful routines for analyzing polynomial ideals, to find the zero sets (varieties) of the obtained polynomial ideals. To obtain the corresponding ideals we used the polar coordinate approach as well as the complexification method for two dimensional polynomial systems (both explained in the following section). It turns out [10] that the isochronicity problem

can be reduced to the linearizability problem, so we can reduce the problem of isochronicity to finding the variety of the ideal generated by (all) linearizability quantities,  $i_{kk}, j_{kk}, k = 1, 2, \dots$ , which are of polynomial dependence on the parameters of (1). On the other hand we can consider directly the isochronicity ideal, generated by coefficients  $T_k$  (which are also of polynomial dependence on the coefficients of (1)). We denote the so called linearizability ideal (generated by all linearizability quantities  $i_{kk}, j_{kk}, k = 1, 2, \dots$ ) by

$$\mathcal{L} = \langle i_{11}, j_{11}, i_{22}, j_{22}, \dots \rangle \quad (3)$$

and  $\mathcal{L}_K = \langle i_{11}, j_{11}, i_{22}, j_{22}, \dots, i_{KK}, j_{KK} \rangle$ . To solve the problem of linearizability means to find an integer  $K \geq 1$  such that  $\mathbf{V}(\mathcal{L}) = \mathbf{V}(\mathcal{L}_K)$  (i.e. the variety of the linearizability ideal equals to the variety of the ideal generated by first  $K$  pairs of linearizability quantities). For this we compute the irreducible decomposition of  $\mathbf{V}(\mathcal{L}_K)$  and using appropriate methods show that all systems from each component of the decomposition are linearizable (implying the obtained conditions being sufficient).

## 2 Definitions

The linear part of system (1) at the origin has two pure imaginary and one non-zero (real) eigenvalue. By definition a  $C^k$ -manifold  $W^c \equiv W^c(0, U)$  in a neighborhood  $U$  of 0 is said to be a *center manifold* of (1) if  $W^c$  is invariant under the flow as long as the solution remains in  $U$  and  $W^c$  is the graph of a  $C^k$ -function  $w = h(u, v)$  which is tangent at 0 to the  $(u, v)$ -space. There is a fundamental theorem (c.f. [2]) which implies that there exists a neighborhood  $U$  of 0 such that there exists a local center manifold  $W^c$  of (1). Note that on any local center manifold,  $w = h(u, v)$ , system (1) becomes a two dimensional (real) system, which can be put in the form

$$\begin{aligned} \dot{u} &= -v + P(u, v), \\ \dot{v} &= u + Q(u, v). \end{aligned} \quad (4)$$

Usually for real two dimensional polynomial systems of the form (4) with maximal degree  $n$  the qualitative analysis is done either by introducing  $x = u + iv$  and  $y = \bar{x} = u - iv$  and obtain the so called *complexification*

$$\dot{x} = x - \sum_{p+q=1}^{n-1} a_{p,q} x^{p+1} y^q, \quad \dot{y} = -y + \sum_{p+q=1}^{n-1} b_{q,p} x^q y^{p+1},$$

for which the linearizability problem is to decide whether the system can be transformed to the linear system  $\dot{X} = X, \dot{Y} = -Y$  by means of a formal change of the plane variables

$$X = x + \sum_{m+j=2}^{\infty} u_{m-1,j}^{(1)}(a, b) x^m y^j, \quad Y = y + \sum_{m+j=2}^{\infty} u_{m,j-1}^{(2)}(a, b) x^m y^j. \quad (5)$$

If such a transformation exists we say that the system is *linearizable*.

Differentiating with respect to  $t$  on both sides of the above two equalities and substituting the complexification in the resulted equalities and then using (5) and the original system (4) yields (after equating coefficients of the same powers) a linear recurrence system for  $u_{m-1,j}^{(1)}$  and  $u_{m,j-1}^{(2)}$ . It turns out (see [10], p. 191) that  $u_{q_1, q_2}^{(1)}$  and  $u_{q_1, q_2}^{(2)}$  can be computed whenever  $q_1 \neq q_2$ . For  $q_1 = q_2 = k \in \mathbb{N}$  some additional (polynomial) conditions, let's say  $i_{kk} = 0$  and  $j_{kk} = 0$  must be fulfilled. The quantities  $i_{kk}$  and  $j_{kk}$  are called *k-th linearizability quantities*. They generate the linearizability ideal defined above.

If  $P$  and  $Q$  in (4) are polynomials of degree at most  $n$  without constant and linear terms, it is convenient to introduce the polar coordinates  $u = r \cos \varphi, v = r \sin \varphi$  and find the so-called *Poincaré return map*  $\mathcal{R}(r)$ , defined by the equation of the trajectories

$$\frac{dr}{d\varphi} = \frac{r^2 F(r, \cos \varphi, \sin \varphi)}{1 + rG(r, \cos \varphi, \sin \varphi)} = R(r, \varphi). \quad (6)$$

The function  $R(r, \varphi)$  is periodic (with the least period  $2\pi$  in variable  $\varphi$ ) and analytic for (small enough)  $|r| < r^*$  (and all  $\varphi$ ); [8]. Thus, we can expand  $R(r, \varphi)$  in a convergent power series in  $r$  to obtain

$$\frac{dr}{d\varphi} = r^2 R_2(\varphi) + r^3 R_3(\varphi) + \dots \quad (7)$$

One can choose (c.f. [8]) the line segment  $\Sigma = \{(u, v); v = 0, 0 \leq u \leq r^*\}$ , where  $r^*$  is chosen to be small enough, to consider the first return of (6) from  $r(\varphi = 0) = r_0$  to  $r(\varphi = 2\pi) = \mathcal{R}(r_0)$ .

Expanding  $r(\varphi, r_0)$  into a (for all  $\varphi \in [0, 2\pi]$  and all  $|r_0| \leq r^*$  convergent) power series in  $r_0$  one obtains

$$r(\varphi, r_0) = w_1(\varphi)r_0 + w_2(\varphi)r_0^2 + w_3(\varphi)r_0^3 + \dots,$$

which is a solution of (7) and inserting  $r(\varphi, r_0)$  into (7) yields recurrence differential equations for functions  $w_j(\varphi)$ , defining the *Poncaré return map*

$$\mathcal{R}(r_0) := r(2\pi, r_0) = r_0 + w_2(2\pi)r_0^2 + w_3(2\pi)r_0^3 + \dots.$$

Obviously, zeros of the difference function  $\mathcal{P}(r_0) = \mathcal{R}(r_0) - r_0$  correspond to closed orbits. In particular, isolated zeros correspond to *limit cycles* and if  $\mathcal{P}(r_0) \equiv 0$  the system has a center at the origin, yielding the conditions  $w_j(2\pi) = 0$  for all  $j > 1$ .

Suppose the origin is center for system (4) and that the number  $r^* > 0$  is so small that the line segment  $\Sigma = \{(u, v); v = 0, 0 \leq u \leq r^*\}$  lies wholly within the period annulus. For  $r$  satisfying  $0 < r < r^*$ , let  $T(r)$  denote the least period of the trajectory through  $(u, v) = (r, 0) \in \Sigma$ . The function  $T(r)$  is the *period function* of the center. If  $T(r)$  is constant, then the center is said to be *isochronous*. It turns out (c.f. [10], p. 176-180) that  $T(r)$  from (2) can be written in the form

$$T(r) = 2\pi\left(1 + \sum_{k=1}^{\infty} p_{2k}r^{2k}\right). \quad (8)$$

Finally, note that any value  $r > 0$  ( $r < r^*$ ) for which  $T'(r) = 0$  is called a *critical period*. When we consider bifurcations of critical periods we are interested in an upper bound of the number of critical periods in small neighborhood of the singular point; it is the so-called problem of *critical period bifurcations*, considered for the first time in [1].

For computing the irreducible decomposition of an ideal a modular approach can be used. The SINGULAR routine (c.f. [3]) `minAssGTZ`, which is based on the algorithm of [6], involves multiple computations of Gröbner bases which are extremely time and memory consuming, especially for large polynomials which is usually the case in computations mentioned above. Thus, the routine `minAssGTZ` very seldom is able to complete computations and return minimal associate primes in cases of non trivial ideals (generated for instance by focus or linearizability quantities or the coefficients,  $T_k$ , of the period function (2)) when computing over the field of rational numbers. To overcome the difficulty the modular approach described in [9] has proved to be very efficient. Following the approach one first computes minimal associate primes over a field  $\mathbb{Z}_p$  of a prime characteristic  $p$  (usually  $p = 32003$  is taken), and then lifts the obtained decomposition to the polynomial ring of characteristic zero using the rational reconstruction algorithm of [11] applied in MATHEMATICA.

### 3 Main results

Edneral et al. [4] studied the dynamics of trajectories at the center manifold for the system (1). They found five conditions for the existence of a center on the center manifold:

1.  $S = 0$ ;
2.  $a = b = c + f = 8c + T^2 - U^2 = 4(e - d) - T^2U^2 = 2(e + d) + TU = 0$  and  $S = 1$ ;
3.  $a = b = c = f = d + e = 0$  and  $S = 1$ ;
4.  $d + e = c = f = T - 2a = U - 2b = 0$  and  $S = 1$ ;
5.  $c = d = e = f = 0$  and  $S = 1$ .

In the sequel, for cases 1. and 4. (defined above) we state some results on isochronicity and critical period bifurcations of a center on the center manifold of (1).

**Case 1.** Obviously  $w = 0$  is a center manifold and the corresponding 2D system is

$$\begin{aligned} \dot{u} &= -v + a(u^2 + v^2), \\ \dot{v} &= u + b(u^2 + v^2). \end{aligned} \quad (9)$$

Isochronicity of (9) was studied in [8] by introducing the polar coordinates. Following the procedure described in the previous section we find that  $T_2 = 2\pi(a^2 + b^2)$ . Thus, we see that the necessary condition for isochronicity of system (9) is  $a = b = 0$ , which, obviously, is also the sufficient condition. To obtain some information about critical periods of system (9) we investigate the derivative,  $T'(r) = 2T_2(a, b)r + 3T_3(a, b)r^2 + \dots$ , of the period function (2). Critical periods of system (9) are zeros of  $T'(r) = 0$ . Recall that series (2) converges for  $r$  small enough. Note that the coefficients  $T_k$  regarded as polynomials in variables  $a$  and  $b$  are homogeneous. Since  $T_2 = 2\pi(a^2 + b^2) > 0$  for all  $(a, b)$  near the origin, by [10], Lemma 6.4.2, we have the following result.

**Theorem 3.1.** *System (9) has an isochronous center if and only if  $a = b = 0$  and no critical periods bifurcate from centers of system (9).*

**Case 4.** On the center manifold  $u^2 + v^2 - w = 0$  (c.f. [4]) the corresponding 2D system reads

$$\begin{aligned}\dot{u} &= -v + (a + dv)(u^2 + v^2), \\ \dot{v} &= u + (b - du)(u^2 + v^2).\end{aligned}\tag{10}$$

The isochronicity problem and the related problem of linearizability seem to be at first glance two different problems. However, according to a theorem of Poincaré and Lyapunov (see e.g. Theorem 4.2.1 in [10]) these two problems are equivalent.

In (10) after substituting

$$a_{11} = b_{11} = d, \quad a_{01} = -b + ia \quad \text{and} \quad b_{10} = -b - ia\tag{11}$$

one obtains system

$$\begin{aligned}\dot{x} &= i(x - a_{11}x^2y - a_{01}xy), \\ \dot{y} &= -i(y + b_{11}xy^2 + b_{10}xy),\end{aligned}\tag{12}$$

where  $a_{kj}, b_{kj} \in \mathbb{C}$ .

We divide by  $i$  and consider  $a_{kj}, b_{kj}$  as independent parameters (not necessary satisfying condition (11)) and  $y$  as an independent unknown function (not necessary satisfying the condition  $y = \bar{x}$ ) and solve the problem of linearizability for this more general system, obtaining the following result.

**Theorem 3.2.** *System (12) is linearizable if and only if one of the following conditions holds:*

- 1)  $a_{01}b_{10} + b_{11} = b_{10} = a_{11} - b_{11} = 0$ ;
- 2)  $a_{01}b_{10} + b_{11} = a_{01} = a_{11} - b_{11} = 0$ .

The Darboux linearization in the proof of the above theorem (see the proof of Th. 2 in [5]) yields the following first two isochronicity quantities for real system (10):

$$\begin{aligned}p_2 &= a^2 + b^2 + d \\ p_4 &= -2(a^2 + b^2)^2.\end{aligned}\tag{13}$$

Now, we obtain some information about critical periods of system (10) investigating the derivative  $T'(r)$  of period function.

**Theorem 3.3.** *If in system (10)*

$$d = -a^2 - b^2\tag{14}$$

*then one critical period bifurcates from the origin after small perturbations.*

*Proof.* Inserting (13) into  $T'(r)$  we obtain

$$T'(r, (a, b, d)) = 2p_2(a, b, d)r + 4p_4(a, b, d)r^3 + \dots\tag{15}$$

Let system (10) with parameters  $a = a^*$ ,  $b = b^*$ ,  $d = d^*$  satisfies condition (14), that is,  $d^* = -a^{*2} - b^{*2}$ . If  $a^{*2} + b^{*2} \neq 0$ , then  $p_4 < 0$ . Choosing  $d > -a^2 - b^2$  and sufficiently small we obtain  $p_2 > 0$  and  $|p_2| \ll |p_4|$ , yielding a system with a small root of  $T'(r)$  near the origin. If  $d = a = b = 0$  then we first perturb the system in such a way that  $d = -a^2 - b^2$  and then apply the perturbation described above, again obtaining a critical period of the period function in a small neighborhood of the origin.  $\square$

**Corollary 3.4.** *System corresponding to the fourth case above has isochronous center if and only if  $a = b = d = 0$ .*

From the real system (10) computing we find  $T_2 = a^2 + b^2 + d$  and  $T_4 = -2(a^2 + b^2)^2$ . By results of [10], p. 287-295, to prove that at most one critical period bifurcates from a center it is sufficient to show that  $T_{2k} \in \langle T_2, T_4 \rangle$  for all  $k > 2$ . However, using its complex form (12) one can prove the equivalent statement, namely:  $p_{2k} \in \langle p_2, p_4 \rangle$  for all  $k > 2$ . In [8], Th. 3.5, the following theorem is proved:

**Theorem 3.5.** *At most one critical period bifurcates from centers on the center manifold of system (10) after small perturbations.*

## Acknowledgments

Authors acknowledge the support of this work by the Slovenian Research Agency. The first author acknowledge also the support by the IMFM, Ljubljana and sincere thanks to professor M. Brešar for the financial support and acknowledge the assistance of professor V.G. Romanovski and thank him sincerely.

## References

- [1] C. Chicone and M. Jacobs. *Bifurcations of critical periods for plane vector fields*. Trans. Amer. Math. Soc., 1989, vol. 312, p. 433–486.
- [2] S. Chow and J. K. Hale, *Methods of Bifurcation Theory*. New York: Springer-Verlag, 1982.
- [3] W. Decker, S. Laplagne, G. Pfister, and H.A. Schönemann, *SINGULAR 3-1 Library for Computing the Primary Decomposition and Radical of Ideals, primdec.lib, 2010*.
- [4] V. F. Edneral, A. Mahdi, V. G. Romanovski and D. S. Shafer, *The center problem on a center manifold in  $R^3$* , Nonlinear Anal., 2012, vol. 75, p. 2614–2622.
- [5] B. Ferčec and M. Mencinger, *Isochronicity of centers at a center manifold*, AIP conference proceedings, 1468. Melville, N.Y.: American Institute of Physics, 2012, p. 148–157.
- [6] P. Gianni, B. Trager, G. Zacharias, *Gröbner bases and primary decomposition of polynomials*, J. Symbolic Comput., 1988, vol. 6, p. 146–167.
- [7] G.M. Greuel, G. Pfister, and H. Schönemann, *SINGULAR 3.0. A Computer Algebra System for Polynomial Computations*, Centre for Computer Algebra, University of Kaiserslautern, 2005; <http://www.singular.uni-kl.de>.
- [8] V. G. Romanovski, M. Mencinger and, B. Ferčec, *Investigation of center manifolds of 3-dim systems using computer algebra*, Program. comput. softw., 2013, vol. 39, no. 2, p. 67–73.
- [9] V.G. Romanovski and M. Prešern, *An Approach to Solving Systems of Polynomials via Modular Arithmetics with Applications*, J. Computational Appl. Math., 2011, vol. 236, p. 196–208.
- [10] V.G. Romanovski and D.S. Shafer, *The Center and Cyclicity Problems: A Computational Algebra Approach*, Boston: Birkhäuser, 2009.
- [11] P.S. Wang, M.J.T. Guy and J.H. Davenport,  *$P$  Adic Reconstruction of Rational Numbers*, SIGSAM Bull., 1982, vol. 16, no. 2, p. 2–3.



# Formal Integral and Caustics in Henon-Heiles model

Tatiana Mylläri, Aleksandr Mylläri  
St. George's University (Grenada)

tmyllari@sgu.edu

## Abstract

We use a formal integral to study the structure of caustics in the Hénon-Heiles model. A Gustavson-like formal integral of motion is used (together with the Hamiltonian of the system) to study analytically the structure of caustics (the structure of the velocity field in the case of projection to the coordinate plane) in the system. Results obtained analytically by using a formal integral of motion are compared with those obtained by the numerical integration.

## Keywords

Hénon-Heiles model, formal integral, caustics in Hamiltonian systems

# Tree structures in Poisson series processors

Juan F. Navarro  
University of Alicante (Spain)

`jf.navarro@ua.es`

## Abstract

Much of the work concerned with the application of perturbation theories in celestial mechanics, and particularly in the development of analytical theories of the motion of celestial bodies, can be reduced to algebraic operations on Poisson series.

The aim of this contribution is to make a review on the use of tree structures for the storage of Poisson series. We analyse a type of structure based on maps, as well as its representation in the form of red–black tree. We also compare the complexity of some fundamental algorithms in their corresponding computer implementation as lists and red–black trees.

## Keywords

Symbolic computation, Poisson series, Maps, Multimaps, Complexity

## 1 Introduction

Since the early sixties, investigators used computers to generate analytical expressions. The first Poisson series processors were born to deal with the theory of the Moon, considered as one of the hardest problems in celestial mechanics. Later, analytical theories for the rotation of the Earth (Kinoshita, 1977) were treated with the help of symbolic computation packages. Nowadays there are many open problems which requires massive symbolic computation.

Many Poisson series processors have been developed until now, as PSP (Broucke, 1970), MAO (Mechanized Algebraic Operations) (Rom, 1969), TRIGMAN (Trigonometric Manipulator) (Jefferys, 1970), MSNam (Henrard, 1986), PARSEC (Richardson, 1989), PSPC (Abad and San–Juan, 1993), and others. We also would like to mention that MSNam software (Manipulateur de Séries de Namur) was first written by H. Claes, J. Henrard, M. Moons and J.M. Zune. It was later improved by M. Moons (1993) and the last version in Fortran 90 was made by J. Henrard in 2004. In this version, the arguments and exponents of the series and the indication that the trigonometric expression is a cosine or a sine are coded and packed in a large array of integers.

Furthermore, several general purpose systems such as Mathematica, Macsyma, Reduce, Maple, Matlab and others have been designed to treat a wide range of problems from many branches of Science. Because of their universality, they are not as efficient as special purpose systems designed for solving some specific applications. In particular, high accuracy analytical problems of celestial mechanics involving perturbation methods require specific symbolic processors.

In this paper, we analyse the red–black tree structure and the way it can be used to represent computationally a Poisson series. This structure leads to best computational times in the basic operations with Poisson series, as addition and multiplication of Poisson series.

## 2 Poisson series as a symbolic object

In this section, we follow F. San–Juan and A. Abad (2001) to introduce the representation of a mathematical object in a computer. We will focus our attention on the set  $\mathcal{P}_{n,m}$  of Poisson series with  $n$  polynomial variables  $x_1, \dots, x_n$ , and  $m$  angular variables  $\phi_1, \dots, \phi_m$ . A Poisson series is a map  $P : \mathbb{R}^n \times \mathbb{R}^m \rightarrow \mathbb{R}$  such that

$$P(x_1, \dots, x_n, \phi_1, \dots, \phi_m) = \sum_{i_1, \dots, i_n} \sum_{j_1, \dots, j_m} C_{i_1, \dots, i_n}^{j_1, \dots, j_m} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n} \frac{\cos}{\sin}(j_1 \phi_1 + \dots + j_m \phi_m), \quad (1)$$

where  $i_1, \dots, i_n, j_1, \dots, j_m \in \mathbb{Z}$ . The set  $\mathcal{P}_{n,m}$ , with the addition of Poisson series and the multiplication of a Poisson series by a real number, is a vectorial space. The partial derivative of a Poisson series with respect to a polynomial or angular variable is also a Poisson series, as well as the multiplication of two Poisson series.

We look for a canonical representation for each equivalence class defined in  $\mathcal{P}_{n,m}$ . For that purpose, the following operations must be performed over each Poisson series:

1. The first non-zero coefficient of the angular variables must be positive. If not, we will apply the following rules:

$$\sin(-\lambda_i \phi_i + \dots) = -\sin(\lambda_i \phi_i - \dots), \quad \cos(-\lambda_i \phi_i + \dots) = \cos(\lambda_i \phi_i - \dots).$$

2. The terms of a Poisson series will be ordered following a lexicographical order, as follows: let us consider two terms of a Poisson series,  $\tau_1$  and  $\tau_2$ , given by

$$\begin{aligned} \tau_1 &= C_{i_1^{(1)}, \dots, i_n^{(1)}}^{i_{n+1}^{(1)}, \dots, i_{n+m}^{(1)}} x_1^{i_1^{(1)}} x_2^{i_2^{(1)}} \dots x_n^{i_n^{(1)}} T^{(1)}(i_{n+1}^{(1)} \phi_1 + \dots + i_{n+m}^{(1)} \phi_m), \\ \tau_2 &= C_{i_1^{(2)}, \dots, i_n^{(2)}}^{i_{n+1}^{(2)}, \dots, i_{n+m}^{(2)}} x_1^{i_1^{(2)}} x_2^{i_2^{(2)}} \dots x_n^{i_n^{(2)}} T^{(2)}(i_{n+1}^{(2)} \phi_1 + \dots + i_{n+m}^{(2)} \phi_m). \end{aligned}$$

We say that  $\tau_1 < \tau_2$  if for the first  $k \in \{1, \dots, n, n+1, \dots, n+m\}$  such that  $i_k^{(1)} \neq i_k^{(2)}$ , then  $i_k^{(1)} < i_k^{(2)}$  is verified or, if for all  $k \in \{1, \dots, n+m\}$ ,  $i_k^{(1)} = i_k^{(2)}$ , and  $T^{(1)} = \cos$  and  $T^{(2)} = \sin$ .

3. The terms of a Poisson series with identical polynomial and angular part must be grouped together.

### 3 Red-black trees and maps

As pointed out in (San-Juan and Abad, 2001), most of the operations involving a series are based on navigating and searching through the structure that represents the series. For example, the addition of two Poisson series is equivalent to insert each term of one series into the other one. Thus, a good choice of the data structure cause simple and efficient algorithms. In this section, we introduce two objects (red-black trees and maps) which have resulted to be very useful in the representation of a Poisson series.

#### 3.1 Red-black trees

The binary tree is a very useful data structure for rapidly storing sorted data and rapidly retrieving saved data. A binary tree is composed of parent nodes, or leaves, each of which stores data and also links to up to two other child nodes (leaves), one of them placed to the left and the other one placed to the right. In this structure, the relationship between the leaves linked to and the linking leaf makes the binary tree an efficient data structure: the leaf on the left has a lesser key value, and the leaf on the right has an equal or larger key value.

A special type of tree is the red-black tree. In a red-black tree, each node has a color attribute, the value of which is either red or black. In addition to the ordinary requirements imposed on binary search trees, the following additional requirements of any valid red-black tree apply:

1. A node is either red or black.
2. The root is black.
3. All leaves are black, even when the parent is black.
4. Both children of every red node are black.
5. Every simple path from a node to a descendant leaf contains the same number of black nodes.

A critical property of red-black trees is enforced by these constraints: the longest path from the root to a leaf is no more than twice as long as the shortest path from the root to a leaf in that tree. The result is that the tree is roughly balanced. Since operations such as inserting,

deleting, and finding values requires worst case time proportional to the height of the tree, this fact makes the red–black tree be an efficient data structure. For instance, the search–time results to be  $O(\log n)$ . As we will discuss later, the use of this structure reduces significantly the complexity of the algorithms for addition and multiplication.

As mentioned above, in a binary tree, each node stores a key value (which must be unique in our case) and some associated data. For every node in the tree, all keys in the left subtree are smaller than the key of the node, and all keys in the right subtree are larger than the key of the node. So, each node is comprised of a key, a value, and a reference to the left (smaller keys) and right (larger keys) subtrees. This means that the key is the way to introduce the lexicographical order in the tree structure.

### 3.2 Maps

A map is an indexed data structure, similar to a vector. However, maps differ from vectors in two important points:

1. In a map, the index values (key values) can be any ordered data type, that is, any data type for which a comparison operator can be defined can be used as a key.
2. A map is an ordered data structure, elements are maintained in sequence, the ordering being determined by key values.

## 4 Poisson series as computational objects

Now, we will consider the basic information which characterizes a Poisson series, as well as the data structure to store it in the computer. This must be done preserving the canonical representation we have chosen. Let us consider a term of a Poisson series,

$$\tau = Cx_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}T(i_{n+1}\phi_1 + \cdots + i_{n+m}\phi_m).$$

The information associated to each term of a Poisson series is given by the following elements:

1. A real number  $C \in \mathbb{R}$  for representing the coefficient of the term.
2. A set of  $n$  integers  $i_1, \dots, i_n \in \mathbb{Z}$  for representing the exponents of the polynomial part.
3. A set of  $m$  integers  $i_{n+1}, \dots, i_{n+m} \in \mathbb{Z}$  for representing the coefficients of the angular part.
4. An integer  $t \in \mathbb{Z}$  ( $t = 0$  if  $T = \cos$  and  $t = 1$  if  $T = \sin$ ).

A Poisson series is computationally considered as a hierarchic structure ordered by a key. This means that the adequate object to store a Poisson series is a map. Each term of the Poisson series corresponds to a node in the map structure. The data associated to each node of the map is a real number representing the coefficient of the corresponding term ( $C$ ), and the key of each node is given by the set  $(i_1, \dots, i_n, i_{n+1}, \dots, i_{n+m}, t)$ .

The most common option for the storage of a Poisson series is the linked list, where each node contains the main characteristics of a separate term of the series. However, the most of the operations involving a series are based on navigating and searching through the structure that represents the series. In order to minimize the searching, deleting and inserting times of a term in a Poisson series, we have adopted the red–black tree as the structure to store a series in the computer. As we have already mentioned above, inserting, deleting, and finding values requires worst case time proportional to the height of the tree. Thus, we will represent a Poisson series as a red–black tree.

Moreover, as pointed out in (San–Juan and Abad, 2011), Poisson series involved in problems of celestial mechanics present small values for indices  $i_1, \dots, i_{n+m}$ , normally in the interval  $[-127, 128]$ . On the other hand, the most of the integers  $i_1, \dots, i_{n+m}$  are zero. These two considerations should be taken into account in the way the structure for the representation of the key of each node, and the series itself, is coded.

If we store the key of a term in a vector structure, and assuming  $n$  and  $m$  polynomial and angular variables respectively, the complexity of the comparison of the keys is  $O(n + m)$ . We can reduce this complexity by storing keys in red–black trees. For each term of a Poisson series, we store

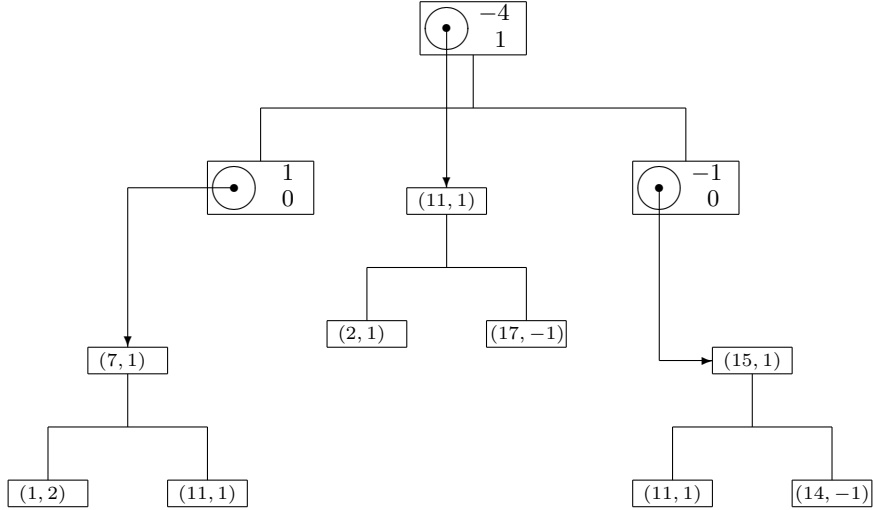


Figure 1: Red–black tree for representing a Poisson series  $P$  belonging to  $\mathcal{P}_{10,12}$ , being  $P = x_1^2 x_7 \cos \phi_1 - 4x_2 \sin(\phi_1 - \phi_7) - \cos(\phi_1 + \phi_5 - \phi_4)$ .

pairs  $(\nu, i_\nu)$  and  $(\nu, j_\nu)$ . Distinction between angular and polynomial variables can be established taking polynomial variables for values of the index between 1 and  $n$ , and angular variables for values of the index between  $n + 1$  and  $n + m$ . Thus, the complexity of comparison between terms is reduced from  $O(n + m)$  to  $O(\log_2(n + m))$  in the worst case scenario.

If the keys associated to two different terms belonging to different Poisson series have different size, that means that both terms are not equal and can not be collected. This fact helps also to reduce the computation time. Moreover, it is not necessary to compare the entire key in case one index fails.

Thus, from a computational point of view, a Poisson series will be represented by a red–black tree with keys stored in red–black trees. In Figure 1, we show the representation of Poisson series

$$P = x_1^2 x_7 \cos \phi_1 - 4x_2 \sin(\phi_1 - \phi_7) - \cos(\phi_1 + \phi_5 - \phi_4),$$

just to clarify the way red–black trees are used to store a Poisson series.

In the following section, we will analyse the complexity of the most basic algorithms to be implemented in a Poisson series processor.

## 5 Basic manipulation of Poisson series

### 5.1 Addition and subtraction of Poisson series

Let us consider two Poisson  $P$  and  $Q$  series containing  $N$  terms each of them. The implementation of this algorithm in a list structure requires: concatenating both lists ( $O(1)$ ), sorting the resulting structure ( $O(N \log_2 N)$ ), and collecting like terms ( $O(N)$ ). The Quicksort algorithm has an average complexity of  $O(N \log_2 N)$ , but in the worst case scenario, the complexity is  $O(N^2)$ , and this case happens when the initial list is already ordered. When adding two Poisson series, both lists are initially sorted after being concatenated. Thus, the resulting list is quasi–sorted, and the complexity of the sorting algorithm results to be closer to  $O(N^2)$  than to  $O(N \log_2 N)$ .

If both series are stored in a red–black tree, addition (or subtraction) of Poisson series implies insertion of each term of  $Q$  in  $P$ : insertion when the key of the term is not contained in  $Q$ , and modification if the key of the term is contained in  $Q$ . In both cases, the complexity is  $O(\log_2 N)$  for each term. Thus, complexity is  $O(N \log_2 N)$ . This algorithm provides the best case when all terms of  $Q$  appear also in  $P$ , with a complexity of  $O(N \log_2 N)$ . In the worst case scenario, the complexity is  $\sum_{i=1}^N \log_2(N + i) = O(N \log_2(N))$ . This occurs when all terms of  $Q$  must be inserted in  $P$  as new elements.

## 5.2 Multiplication of Poisson series

Let us consider two Poisson series  $P$  and  $Q$  with  $N_P$  and  $N_Q$  terms respectively. The multiplication of these two series can adopt the form of a Poisson series taking into account the following relations:

$$\begin{aligned} 2 \cos \lambda \cos \mu &= \cos(\lambda + \mu) + \cos(\lambda - \mu), & 2 \sin \lambda \sin \mu &= \cos(\lambda - \mu) - \cos(\lambda + \mu), \\ 2 \sin \lambda \cos \mu &= \sin(\lambda + \mu) + \sin(\lambda - \mu), & 2 \cos \lambda \sin \mu &= \sin(\lambda + \mu) - \sin(\lambda - \mu), \end{aligned}$$

which can be applied when  $\lambda = i_{n+1}\phi_1 + \dots + i_{n+m}\phi_m$  and  $\mu = i'_{n+1}\phi_1 + \dots + i'_{n+m}\phi_m$ . The implementation of this algorithm with a list structure has a complexity of  $O(N^2M^2(n+m))$ . For each term of series  $P$ , we have to visit each term in  $Q$  and then, compute and insert the resulting terms in the product series.

If we use a structure base on red–black trees, the cost of the insertion is then  $\log_2(NM)$  instead of  $NM$ . So, the total complexity is reduced to  $O(NM \log_2(NM) \log_2(n+m))$ .

## 6 Conclusions

We have analysed how the adoption of a red–black tree structure to store Poisson series can reduce the computational cost of basic algorithms, as addition and multiplication of Poisson series. This structure leads to best computational times because basic operations like searching, insertion and deletion have logarithmic cost.

## References

- [1] Abad, A., San-Juan, J. F. PSPC, A Poisson series processor coded in C. *Dynamics and Astrometry of Natural and Artificial Celestial Bodies*, Poznan, Poland, pp. 383-389.
- [2] Broucke, R. How to assemble a Keplerian processor, *Celest. Mech.*, 2, 9–20 (1970)
- [3] Henrard, J. Algebraic manipulation on computers for lunar and planetary theories, *Proceedings of the IAU Symposium*, 114, Reidel Kovalevsky, J. and Brumberg, V. (eds.), 59–62 (1986)
- [4] Jefferys, W. H. A Fortran–based list processor for Poisson series, *Celest. Mech.*, 2, 474–480 (1970)
- [5] Kinoshita, H. Theory of the rotation of the rigid Earth, *Celest. Mech.*, 15, 277–326 (1977)
- [6] Moons, M. Averaging approaches, *Proceedings of the “Artificial Satellite Theory Workshop”*, USNO, Washington, DC, 201 (1993)
- [7] Richardson, D. L. PARSEC: An interactive Poisson series processor for personal computing systems, *Celest. Mech. Dyn. Astron.*, 45, 267–274 (1989)
- [8] Rom, A. Mechanized algebraic operations (MAO), *Celest. Mech.*, 1, 301–319 (1969)
- [9] San-Juan, F. and Abad, A. Algebraic and Symbolic Manipulation of Poisson Series, *J. Symbolic Computation*, 32, 565–572 (2001)

# Normal Forms of Singular Plane Quartics

Tadashi Takahashi  
Konan University (Japan)

takahasi@konan-u.ac.jp

## Abstract

It is well-known that a variety of moduli of singular plane quartics has the dimension which is not greater than five. We will show the process which get the normal forms and try to construct normal forms for homogeneous polynomials of the defining equations. And moreover we show their restrictions by using the Gröbner basis of the elimination ideal.

Let  $M\text{-dim}_f$  be the dimension of variety of moduli of the curve defined by the normal form. Then we obtain the following 23 types of forms as the normal forms of irreducible singular plane quartics.

Type	$M\text{-dim}_f(A)$	Total sum of sing.(B)	A + B
$\text{III}_n$	5	1	6
$\text{III}_l$	4	2	6
$\text{III}_g$	3	3	6
$\text{III}_n$	4	1	5
$\text{III}_l$	3	2	5
$\text{III}_g$	2	3	5
$\text{III}_m$	4	2	6
$\text{III}_d$	0	6	6
$\text{III}_e$	1	5	6
$\text{III}_j$	2	4	6
$\text{III}_f$	2	4	6
$\text{III}_k$	3	3	6
$\text{III}_i$	3	3	6
$\text{III}_b$	1	5	6
$\text{III}_c$	2	4	6
$\text{III}_h$	2	4	6
$\text{III}_a$	1	5	6
$\text{II}_{\frac{1}{2}b}$	0	6	6
$\text{II}_a$	1	5	6
$\text{I}_a$	0	6	6
$\text{II}_{\frac{1}{2}a}$	2	4	6
$\text{II}_b$	1	5	6
$\text{I}_b$	0	6	6

For all types of the above irreducible singular plane quartics,  $(M\text{-dim}_f) + (\text{Total sum of Milnor numbers of the singularities}) = 6$  or  $5$ .

## Keywords

Singular plane quartics, Normal forms, Gröbner Basis





---

# Session 3: Algebraic and Algorithmic Aspects of Differential and Integral Operators Session

---

Organizers:

Moulay Barkatou  
Thomas Cluzeau  
Georg Regensburger  
Markus Rosenkranz



# Seeking recursion operators – an universal hierarchy example in dimension $(2 + 1)$

Hynek Baran  
Silesian University in Opava (Czech Republic)

hynek.baran@math.slu.cz

## Abstract

Integrability is one of the key notions in the theory of nonlinear partial differential equations. Although several definitions may be given, the commonly accepted sign of integrability is the existence of an infinite hierarchy of (possibly nonlocal) symmetries and/or conservation laws of the equation in question. Such a hierarchy may be revealed by the use of the (local or nonlocal) recursion operator, which also may be considered as an attribute of the integrability.

In this talk, we focus on the  $(2 + 1)$ -dimension universal hierarchy [3] equations of the form

$$u_{tx} = u_{xy}u_y - u_{yy}u_x$$

discussed in [5], resp.

$$u_{yy} = u_y u_{tx} - u_x u_{ty}$$

investigated by [4].

According to [2] technique, an algorithmic approach to seek for recursion operators, which is applicable to nonlinear PDE's or systems regardless of the number of space variables, we used Jets library [1] to find recursion operators and appropriate nonlocal structures of the equations above.

To obtain the result, heavy computations were run, owing to support of parallelism in Jets, partially distributed to a simple computer cluster, which arrangement we briefly discuss. In comparison to  $(1 + 1)$  dimension, there is an extreme increase in memory usage (dozens of gigabytes) and processor time (a few weeks) consumption.

## Keywords

Nonlinear partial differential equation, integrability, symmetry, conservation law, recursion operator, JETS, distributed computing

## References

- [1] Hynek Baran, Michal Marvan, Jets. A software for differential calculus on jet spaces and diffieties. <http://jets.math.slu.cz>
- [2] Iosif Krasil'shchik, Alexander Verbovetsky, Raffaele Vitolo, A unified approach to computation of integrable structures, arXiv:1110.4560 [nlin.SI]
- [3] Martínez Alonso L., Shabat A.B., Hydrodynamic reductions and solutions of a universal hierarchy. Theor. Math. Phys., 2004,140, 10731085
- [4] Oleg I. Morozov, A Recursion Operator for the Universal Hierarchy Equation via Cartan's Method of Equivalence, arXiv:1205.5748 [nlin.SI]
- [5] Valentin Ovsienko, Bi-Hamiltonian nature of the equation  $u_{tx} = u_{xy}u_y - u_{yy}u_x$ , arXiv:0802.1818 [nlin.SI]

# The algebra of polynomial integro-differential operators and its group of automorphisms

Vladimir Bavula

University of Sheffield (UK)

v.bavula@sheffield.ac.uk

## Abstract

The talk is about general properties of the algebra of polynomial integro-differential operators  $\mathbb{I}_n := K\langle x_1, \dots, x_n, \frac{\partial}{\partial x_1}, \dots, \frac{\partial}{\partial x_n}, \int_1, \dots, \int_n \rangle$ .

We show that the algebra  $\mathbb{I}_n$  is a prime, central, catenary, self-dual, non-Noetherian algebra of classical Krull dimension  $n$  and of Gelfand-Kirillov dimension  $2n$ . Its weak dimension is  $n$ , and  $n \leq \text{gl.dim}(\mathbb{I}_n) \leq 2n$ . All the ideals of  $\mathbb{I}_n$  are found explicitly, there are only finitely many of them ( $\leq 2^{2^n}$ ), they commute ( $\mathfrak{a}\mathfrak{b} = \mathfrak{b}\mathfrak{a}$ ) and are idempotent ideals ( $\mathfrak{a}^2 = \mathfrak{a}$ ). An analogue of the Hilbert's Syzygy Theorem is proved for  $\mathbb{I}_n$ . The group of units of the algebra  $\mathbb{I}_n$  is described (it is a huge group). A canonical form is found for each integro-differential operators (by proving that the algebra  $\mathbb{I}_n$  is a generalized Weyl algebra). All the mentioned results hold for the Jacobian algebra  $\mathbb{A}_n$  (but  $\text{GK}(\mathbb{A}_n) = 3n$ , note that  $\mathbb{I}_n \subset \mathbb{A}_n$ ). It is proved that the algebras  $\mathbb{I}_n$  and  $\mathbb{A}_n$  are ideal equivalent.

The group  $G_n$  of automorphisms of the algebra  $\mathbb{I}_n$  is found:

$$G_n = S_n \times \mathbb{T}^n \times \text{Inn}(\mathbb{I}_n) \supseteq S_n \times \mathbb{T}^n \times \underbrace{\text{GL}_\infty(K) \times \dots \times \text{GL}_\infty(K)}_{2^n - 1 \text{ times}},$$

$$G_1 \simeq \mathbb{T}^1 \times \text{GL}_\infty(K),$$

where  $S_n$  is the symmetric group,  $\mathbb{T}^n$  is the  $n$ -dimensional torus,  $\text{Inn}(\mathbb{I}_n)$  is the group of inner automorphisms of  $\mathbb{I}_n$  (which is huge). It is proved that each automorphism  $\sigma \in G_n$  is uniquely determined by the elements  $\sigma(x_i)$ 's or  $\sigma(\frac{\partial}{\partial x_i})$ 's or  $\sigma(f_i)$ 's. The stabilizers in  $G_n$  of all the ideals of  $\mathbb{I}_n$  are found, they are subgroups of *finite* index in  $G_n$ . It is shown that the group  $G_n$  has trivial centre. For each automorphism  $\sigma \in G_n$ , an *explicit inversion formula* is given via the elements  $\sigma(\frac{\partial}{\partial x_i})$  and  $\sigma(f_i)$ .

## Keywords

The algebras of polynomial integro-differential operators, the group of automorphisms, the canonical form, the Jacobian algebras.

# Darboux theory of integrability in the sparse case

Guillaume Chèze

Institut de Mathématiques de Toulouse, CNRS

guillaume.cheze@math.univ-toulouse.fr

## Abstract

In 1878, G. Darboux has given a strategy to find first integrals of a derivation  $D = \sum_{i=1}^n A_i(X_1, \dots, X_n) \partial_{X_i}$ . One of the tools developed by G. Darboux is now called *Darboux polynomials*.

A polynomial  $f$  is said to be a *Darboux polynomial*, if  $D(f) = g.f$ , where  $g$  is a polynomial. The polynomial  $g$  is called the cofactor.

G. Darboux has shown that if the derivation  $D$  has degree  $d$  and at least  $\binom{n+d-1}{n} + 1$  irreducible Darboux polynomials then  $D$  has a first integral which can be expressed by means of these polynomials.

In 1979, J.-P. Jouanolou has proved, that if a derivation has at least  $\binom{n+d-1}{n} + n$  irreducible Darboux polynomials then the derivation has a rational first integral. We recall that a rational first integral is a first integral which belongs to  $\mathbb{C}(X_1, \dots, X_n)$ .

These results are given in terms of the degree of the polynomial vector field. Here we show that we can get the same kind of results if we consider the size of a Newton polytope associated to the vector field. We recall that the Newton polytope of a Laurent polynomial  $f(\underline{X}) = \sum_{\alpha} c_{\alpha} X^{\alpha}$ , where  $\underline{X} = X_1, \dots, X_n$  and  $\alpha$  is a multi-index  $(\alpha_1, \dots, \alpha_n) \in \mathbb{Z}^n$ , is the convex hull in  $\mathbb{R}^n$  of the exponent  $\alpha$  of all nonzero terms of  $f$ . We denote this polytope by  $\mathcal{N}(f)$ .

**Theorem 1.** *Let  $D = \sum_{i=1}^n A_i(X_1, \dots, X_n) \partial_{X_i}$  be a derivation. Consider generic values  $(x_1, \dots, x_n)$  in  $\mathbb{C}^n$  and the polytope  $N_D = \mathcal{N}\left(\sum_{i=1}^n x_i \frac{A_i}{X_i}\right)$ .*

*Let  $B$  be the number of integer points in  $N_D \cap \mathbb{N}^n$ , then*

- if  $D$  has at least  $B + 1$  irreducible Darboux polynomials then  $D$  has a first integral,*
- if  $D$  has at least  $B + n$  irreducible Darboux polynomials then  $D$  has a rational first integral. Furthermore, this bound is optimal.*

We can remark that this result gives the classical bounds in the dense case.

## Keywords

Darboux theory of integrability, Newton polytope

# Isomorphisms and Serre's reduction of linear functional systems

Thomas Cluzeau

Université de Limoges ; CNRS ; XLIM UMR 7252, DMI (France)

Alban Quadrat

Inria Saclay - Île-de-France, DISCO project, L2S, Supelec (France)

`cluzeau@ensil.unilim.fr`

## Abstract

Within the algebraic analysis approach to linear systems theory, a behaviour is the dual of the left module finitely presented by the matrix of functional operators defining the linear functional system. In this talk, we give an explicit characterization of isomorphic finitely presented modules, i.e., of isomorphic behaviours, in terms of certain inflations of their presentation matrices. Fitting's theorem (see [3] and references therein) on the syzygy modules can be found again. If one of the presentation matrix has full row rank, this result yields a characterization of isomorphic modules as the completion problem characterizing Serre's reduction, i.e., the possibility to find a presentation of the module defined by fewer generators and fewer relations, and thus an equivalent representation of the behaviour defined by fewer equations in fewer unknown functions (see [1] and references therein). This completion problem is shown to induce different isomorphisms between the modules finitely presented by the matrices defining the inflations. Applications to doubly coprime factorizations are given. Finally, we will show that Serre's reduction implies the existence of a certain idempotent endomorphism of the finitely presented module, i.e., a particular decomposition problem (see [2]), proving the converse of a result obtained in [4].

## Keywords

Multidimensional linear systems, algebraic analysis, isomorphic  $D$ -modules, Serre's reduction

## References

- [1] M. S. Boudelloua, A. Quadrat, Serre's reduction of linear functional systems, *Math. Comput. Sci.* 4, 289-312, 2010.
- [2] T. Cluzeau, A. Quadrat, Factoring and decomposing a class of linear functional systems, *Linear Algebra Appl.* 428, 324-381, 2008.
- [3] T. Cluzeau, A. Quadrat, A constructive version of Fitting's theorem on isomorphisms and equivalences of linear systems', *Proceedings of nDS'11*, Poitiers, France, 2011.
- [4] T. Cluzeau, A. Quadrat, Further results on the decomposition and Serre's reduction of linear functional systems, *Proceedings of the 5<sup>th</sup> Symposium on System Structure and Control*, IFAC Worskhop, Grenoble (France), (04-06/02/13).

# Qualitative Study of Polynomial Differential Systems

Dahira Dali, Abderrahmane Turki  
University of science and technology Houari Boumediene (Algeria)

Faculty of mathematics  
Laboratory of Arithmetic, Coding, Combinatorics and Symbolic Computation

dddahira@gmail.com

## Abstract

We develop an algorithmic method based on Gröbner bases in qualitative study of polynomial differential systems with coefficients in a field of characteristic zero. We will give examples in the case of quadratic differential systems.

## Keywords

Polynomial differential systems, invariant, covariant, qualitative study, Gröbner bases, generators system, linear transformations, normal form.

## 1 Motivation

The polynomial differential systems are objects of numerous scientific investigations . They play a prominent role in medicine, biology, engineering, physics, economics, and other disciplines. The invariant theory [7, 11, 6] is one of the most important tools used in the qualitative study of polynomial differential systems. This theory allows to characterize geometric properties of a given differential systems under the action of a given linear group of transformations, with the help of algebraic or semi-algebraic relations depending on the coefficients of these systems. Thus the theory of invariants is proven useful in the qualitative studies of polynomial differential systems, in particular to establish invariant conditions in relation to the given group of transformations, that give the existence and the nature of singular points, and characterize normal forms or the number of complete curves etc. The Einsteins notation [14] in the polynomial differential systems played an important role in the qualitative survey of these systems. In the case where the algebra of invariants is of finite type, the Aronhold identities [11] based on the fondamental theorem of the ivariants with respect to the general linear group and using computation of determinants, gives us a symbolic method to express invariants [14]. In [2] one give an alternative method based on the test of membership in an ideal using Groebner bases and in [3] one develop an algorithmic method to describe the algebra of the algebraic invariants with respect to the general linear group. The computation of invariants, however still difficult. Indeed, even for planar quadratic differential systems, the invariants are polynomials of 12 indeterminates. The Computer algebra Become an indispensable means when using the theory of invariants. Indeed, the qualitative study of polynomial differential systems leads on algebraic systems. Groebner basis is one of the main practical tools for solving systems of polynomial equations and computing algebraic varieties [5]. Many works are devoted to solving algebraic systems ([8, 9, 12]). The spectacular progress of the computer algebra and the efficient of the software( Maple, Magma, Singular etc) motivate our work. Our aim is to show the role of Gröbner bases in qualitative study of the differential polynomial systems. One give examples in the case of planar quadratic systems.

## 2 Preliminaries

Using Einstein's notation (see e.g. [14]), the complete polynomial differential systems of finite dimension  $n$  and of degree at most  $k$  with coefficients in a field  $\mathbb{k}$  of characteristic zero can be

written as

$$\frac{dx^j}{dt} = a^j + a_{\alpha_1}^j x^{\alpha_1} + a_{\alpha_1 \alpha_2}^j x^{\alpha_1} x^{\alpha_2} + a_{\alpha_1 \dots \alpha_r}^j x^{\alpha_1} \dots x^{\alpha_r}, \quad j, \alpha_1, \alpha_r \in \{1, \dots, n\}, 1 \leq r \leq k, \quad (1)$$

where for  $j = 1, \dots, n$  and for  $2 \leq r \leq k$ , the tensor  $a_{\alpha_1 \dots \alpha_r}^j$  (1 time contravariant and  $r$  times covariant) is symmetric with respect to the lower subscripts. Let  $S$  be the set of all coefficients on the right hand side and  $x = (x^1, \dots, x^n)$  be the vector of the unknown variables of (1). Let  $G$  be a group of linear transformations of the phase space  $\mathbb{k}^n$  of the systems (1). The group can be the general linear group  $GL(n, \mathbb{k})$ , the group of translations  $T(n, \mathbb{k})$  or their product  $T(n, \mathbb{k}) \times GL(n, \mathbb{k})$ . When using the invariant theory in the qualitative study of differential systems we transform these systems to systems whose coefficients are invariant with respect to the linear group.

## 2.1 Definition

A polynomial function  $C : S \times \mathbb{k}^n \rightarrow \mathbb{k}$  is a covariant with respect to the group  $G$ , or  $G$ -covariant if there exists a character  $\lambda$  of the group  $G$ , such that  $\forall q \in G, \forall a \in S, C(\rho(q)a, qx) = \lambda(q)C(a, x)$ , where  $\rho$  is a representation of the considered group. If  $\lambda \equiv 1$ , the covariant is said to be absolute, otherwise it is said to be relative. In the case of the linear group  $GL(n, \mathbb{k})$ ,  $\lambda(q) = \det(q)^{-\varkappa}$ , where  $\varkappa$  is an integer ([7, 14]) called the weight of the covariant  $C(a, x)$ . If the polynomial  $C(a, x)$  is independent of  $x$ , then it is said to be a  $G$ -invariant.

## 2.2 Definition

A  $G$ -covariant  $C(a, x)$  is said to be reducible if it can be expressed as a polynomial function of  $G$ -covariants of lower degree. If  $C(a, x)$  is reducible, we write  $C(a, x) \equiv 0$  (modulo  $G$ -covariants of lower degree).

## 2.3 Definition

A finite family  $B$  of  $G$ -covariants of (1) is called a system of generators if any  $G$ -covariant of (1) can be expressed as a sum of products of constants and elements in  $B$ .

## 2.4 Definition

A finite family  $B$  of  $G$ -covariants of the system (1) is a system of generators of the  $G$ -covariants of the system if every  $G$ -covariant of (1) is reducible to zero modulo  $B$ .

## 2.5 Definition

A system  $B$  of generators is said to be minimal if none of them is generated by the others.

The  $GL(n, \mathbb{k})$ -covariants of (1) are called central-affine covariants. One recall the two fundamental results about central-affine invariants.

## 2.6 Theorem([11])

The algebra  $k[x]^{GL(n, \mathbb{k})}$  of central-affine covariants of (1) is of finite type.

## 2.7 Theorem of Gurevich([10])

Any system of generators of central-affine covariants of (1) is made up of polynomial expressions of the coefficients of these systems and the vector  $x$  obtained from the tensorial operations of alternation or total contraction.

# 3 Groebner Bases of Central-Affine Covariants

## 3.1 Corollary

A central-affine covariant  $C$  of differential systems (1) is a tensor of

$$(\mathcal{T}_0^1)^{\otimes d_0} \otimes (\mathcal{T}_1^1)^{\otimes d_1} \otimes \dots \otimes (\mathcal{T}_s^1)^{\otimes d_r} \otimes \mathbb{k}^{\otimes \delta}, \quad 1 \leq r \leq k,$$



obtained from alternation or total contraction, where for  $r = 1, \dots, k$ ,  $\mathcal{T}_r^1$  denotes the space of tensors 1 time contravariant and  $r$  times covariants. ( $\mathcal{T}_r^1$  corresponds to the homogenous part of degree  $r$  of the polynomials of the right hand side of systems (1)).

This corollary is the consequence of the fundamental theorem of Gurevich. It motivates the following definitions.

### 3.2 Definition

A central-affine covariant of (1) is said to be of type  $(d_0, d_1, \dots, d_r, \delta)$  if it is homogeneous of degree  $d_0$  in relation to  $a^j$ , of degree  $d_1$  in relation to  $a_{\alpha_1}^j$ , ..., of degree  $d_r$  in relation to  $a_{\alpha_1 \dots \alpha_r}^j$  and of degree  $\delta$  in relation to the contravariant vector  $x$ .

#### 3.2.1 Examples

$I = a_{\alpha}^{\alpha}$  the trace of the matrix  $a$  which corresponds to the linear part of (1),  $J = a_{pr}^{\alpha} a_{\beta q}^{\beta} a_{\gamma s}^{\gamma} a_{\alpha \delta}^{\delta} \varepsilon^{pq} \varepsilon^{rs}$  (where  $\varepsilon^{pq} = q - p$ ,  $\varepsilon^{rs} = s - r$  and  $n = 2$ ) are central-affine covariants of (1) of type  $(0, 1, 0, \dots, 0)$  and  $(0, 0, 4, \dots, 0)$ , respectively.

### 3.3 Definition

A monomial associated with (1) is a finite product of the form

$$(a^j)^{p_0} (a_{\alpha_1}^j)^{p_1} (a_{\alpha_1 \alpha_2}^j)^{p_2} \dots (a_{\alpha_1 \dots \alpha_r}^j)^{p_r} x^{\alpha}, \quad 1 \leq r \leq k$$

where for  $\alpha = (\delta_1, \dots, \delta_n) \in \mathbf{N}^n$ ,  $x^{\alpha}$  denotes the product  $(x^1)^{\delta_1} \dots (x^n)^{\delta_n}$ .

We define on the set of all monomials denoted by  $\mathcal{M}$  the usual product.

$$\begin{aligned} & (a^j)^{p_0} (a_{\alpha_1}^j)^{p_1} (a_{\alpha_1 \alpha_2}^j)^{p_2} \dots (a_{\alpha_1 \dots \alpha_r}^j)^{p_r} x^{\delta} \times (a^j)^{q_0} (a_{\alpha_1}^j)^{q_1} (a_{\alpha_1 \alpha_2}^j)^{q_2} \dots (a_{\alpha_1 \dots \alpha_r}^j)^{q_r} x^{\mu} \\ = & (a^j)^{p_0+q_0} (a_{\alpha_1}^j)^{p_1+q_1} (a_{\alpha_1 \alpha_2}^j)^{p_2+q_2} \dots (a_{\alpha_1 \dots \alpha_r}^j)^{p_r+q_r} x^{\delta+\mu} \end{aligned}$$

By treating the tensorial coefficients as ‘alphabets’, one define a total lexicographic ordering for the set  $\mathcal{M}$  in the usual manner (see e.g. [15, pp. 373-375]). It’s easy to verify the following theorem.

### 3.4 Theorem

For any polynomial differential system (1) the ideal of central-affine covariants of these systems has a Gröbner basis.

Let  $\mathcal{F}$  be a given system of generators of the ideal  $\mathcal{I}$  of central-affine covariants of (1). The Hilbert’s basis theorem implies that  $\mathcal{F}$  is finite. The fundamental theorem of the central-affine covariants of (1) offer us a constructive method to compute this generating family. Starting from  $\mathcal{F}$  using the Buchberger’s criterion [5] one construct a groebner basis of this ideal denoted  $\mathcal{B}$ .  $\mathcal{B}$  will be said groebner basis of central-affine covariants of (1).

## 4 Qualitative Study of Polynomial Differential Systems

The action of the group  $GL(n, \mathbb{k})$  on  $\mathbb{k}^n : (q, x) \mapsto qx$ , induces a representation of group,

$$\rho : GL(n, \mathbb{k}) \longrightarrow GL(S)$$

defined by  $\rho(q)(a^j) = q_i^j a^i$  and  $\rho(q)(a_{\alpha_1 \dots \alpha_r}^j) = q_i^j p_{\alpha_1}^{j_1} \dots p_{\alpha_r}^{j_r} a_{j_1 \dots j_r}^i$  where  $j, \alpha_1, \dots, \alpha_r \in \{1, \dots, n\}$ ,  $r = 1, \dots, k$ , and  $q$  is a matrix of  $GL(n, \mathbb{k})$  and  $p$  its inverse.

Let  $q$  be a given matrix in  $GL(n, \mathbb{k})$ . Systems (1) can be transformed into the following systems,

$$\frac{dx^j}{dt} = b^j + b_{\alpha_1}^j x^{\alpha_1} + b_{\alpha_1 \alpha_2}^j x^{\alpha_1} x^{\alpha_2} + b_{\alpha_1 \dots \alpha_r}^j x^{\alpha_1} \dots x^{\alpha_r}, \quad j, \alpha_1, \alpha_r \in \{1, \dots, n\}, 1 \leq r \leq k, \quad (2)$$

where for  $j = 1, \dots, n$  and for  $2 \leq r \leq k$ ,  $b^j = \rho(q)(a^j)$  and  $b_{\alpha_1 \dots \alpha_r}^j = \rho(q)(a_{\alpha_1 \dots \alpha_r}^j)$ .

Starting from systems (2) we characterise normal forms of the given differential systems (1). We illustrate our idea by mean of the complete planar quadratic differential systems.

$$\frac{dx^j}{dt} = a^j + a_{\alpha_1}^j x^{\alpha_1} + a_{\alpha_1 \alpha_2}^j x^{\alpha_1} x^{\alpha_2}, \quad j, \alpha_1, \alpha_2 \in \{1, 2\} \quad (3)$$

The ideal of the central-affine covariants of these systems is generated [1, 14] by the family  $\mathcal{F} = \{I_1, \dots, I_{16}, K_1, \dots, K_{33}\}$ .

#### 4.1 proposition

If  $I_9 \neq 0$  the systems (3) can be transformed into new polynomial differential systems with invariant coefficients with respect to the group  $GL(n, R)$ .

Indeed, under the matrix  $q$  defined by  $q_u^\alpha = a_{\alpha u}^\alpha$  and  $q_u^\beta = \frac{1}{I_9} a_{\alpha r}^\alpha a_{su}^\beta a_{\beta \gamma}^\gamma \varepsilon^{rs}$  the systems (3) can be transformed into the systems

$$\frac{dx^j}{dt} = b^j + b_{\alpha_1}^j x^{\alpha_1} + b_{\alpha_1 \alpha_2}^j x^{\alpha_1} x^{\alpha_2}, \quad j, \alpha_1, \alpha_2 \in \{1, 2\} \quad (4)$$

where coefficients of the new systems (4) are depending on the coefficients of the systems (3) and the elements of the matrix  $q$ . It's easy to check with the help of the definition of central-affine covariants that the new coefficients are invariant. Since  $I_1, \dots, I_{36}$  are still invariant under any centro-affine transformation, they are invariant under the transformation  $q$ . Hence, We may compute

$$I_1 = b_1^1 + b_2^2, I_3 = b_1^2 b_{22}^2 - b_2^1 b_{11}^1, I_4 = -b_2^1, I_7 = b_{22}^1 (b_{11}^1 - b_{22}^2), I_9 = b_{22}^1,$$

$$I_{13} = b_{22}^1 (b_2^2 b_{12}^2 - b_1^1 b_{11}^1), I_{15} = -(b_{22}^1)^2 b_{11}^1, I_{17} = b^1, I_{26} = b^2 b_{22}^1. \quad (5)$$

We follow the idea in [14, Lemma 17.2], and then solve for

$$b^1 = I_{17}, b^2 = \frac{I_{26}}{I_9}, b_1^1 = \frac{I_1(I_9 - I_7) - 2I_{13}}{2I_9}, b_2^1 = -I_4, b_1^2 = \frac{2I_3 I_9 - I_4(I_7 + I_9)}{2I_9^2}, b_2^2 = \frac{I_1(I_7 + I_9) + 2I_{13}}{2I_9},$$

and

$$b_{11}^1 = \frac{I_7 + I_9}{2I_9}, b_{12}^1 = 0, b_{22}^1 = I_9, b_{11}^2 = -\frac{I_{15}}{I_9^2}, b_{12}^2 = \frac{I_9 - I_7}{2I_9}, b_{22}^2 = 0.$$

which are invariant and then they determinate a normal form of the quadratic systems (3) since all the new coefficients are expressed in terms of  $\{I_1, \dots, I_{26}\}$  of elements of our generating family  $\mathcal{F}$ . Then we are able to study these differential systems with the help of the invariant theory.

Let return to our differential systems (1). Starting from a generating family  $\mathcal{F} = \{f_1, \dots, f_s\}$  of the ideal of the central-affine covariants of these systems one compute a groebner basis  $\mathcal{B}$ , using an appropriate monomial order. One choose an invertible matrix which transforms systems (1) into new systems (2) which coefficients are invariant under the action of the linear group and compute each element of  $\mathcal{F}$  in terms of the new coefficients of the transformed systems and then lead to an algebraic system of at most  $s$  equations,

$$f_1 = P_1(b^1, \dots, b_{n, \dots, n}^n), \dots, f_s = P_s(b^1, \dots, b_{n, \dots, n}^n). \quad (6)$$

where the indetrminates are the new coefficients of the transformed systems (2). A normal form is obtained by solving (6), then expressing each new coefficient in the ideal  $\langle \mathcal{F} \rangle$ . Now we are able to give an algorithm that determinates a normal form of a given system (1).

#### 4.2 Algorithm

- Step 1. Enter an invertible matrix  $q$  and a finite generating family  $\mathcal{F} = \{f_1, f_2, \dots, f_s\}$  of central-affine covariants of (1)
- Step 2. Order  $\mathcal{M}$  by a monomial order.
- Step 3. Deduce from  $\mathcal{F}$  a groebner basis  $\mathcal{B}$
- Step 4. Transform the systems (1) under the matrix  $q$  into new systems (2).

- Step 5. If the new coefficients are central-affine covariant go to step 6 else choose another matrix and go to step 1.
- Step 6. Compute the elements of the generating family  $\mathcal{F}$  in terms of the new coefficients of systems (2) then lead to the algebraic system (6).
- Step 7. Express the new coefficients in  $\langle \mathcal{F} \rangle$  when solving (6) with the help of groebner basis.
- Step 8. Return a normal form.

## 5 Conclusion

The computation of invariants of differential polynomial systems (1) is not easy. However, the Groebner bases can play a role in the development of the qualitative study of differential systems of finite dimension with coefficients in a field of characteristic zero, with the help of an efficient software. It'll be interesting to develop an algorithm using groebner bases to study the existence and the nature of singular points for a given polynomial differential system with coefficients in the field of the complex numbers, the cubic systems for example.

## References

- [1] Driss Boularas and Dahira Dali, Sur les bases de concomitants centro-affines des systèmes différentiels, Cahiers Mathématiques d'Oran, 1987, no. 2, 25-30.
- [2] Dahira Dali, Gröbner Bases of algebraic invariants in polynomial differential systems, LE MATEMATICHE, Vol LXIII (2008)- Fasc. II, pp. 16-21.
- [3] Dahira Dali and Sui Sun Cheng Decomposition of Central-Affine Covariants of Polynomial Differential Systems, Taiwanese J. Math. 14, No. 5, 1903-1924 (2010). ISSN 1027-5487.
- [4] N. I. Danilyuk and C. S. Sibirskii, Syzygies between central-affine invariants of a quadratic differential system, Differentsialnyje Uravnenija, Vol 17(2)(1981), 210-219.
- [5] David Cox John Little Daniel OShea, Ideals Varieties and Algorithms, Springer 2007.
- [6] H. Derksen, H. Kraft, Constructive Theory, Collection Algèbre non commutative, Groupes quatiques et invariants, Smin. Cong.2(1995)? SMF, 221-224.
- [7] J. Dieudonné and J. Carrell, Invariant theory, old and new, Adv. in Math., 4(1970), 1-80.
- [8] Faugre, J.-C. (June 1999). A new efficient algorithm for computing Grbner bases (F4). Journal of Pure and Applied Algebra (Elsevier Science) 139 (1): 6188.
- [9] Marc Giusti, Luis Miguel Pardo Algorithms for Polynomial Ideals and their Varieties, Computer Algebra Handbook, Johannes Grabmeir, Eric Kaltofen and Volker Weispfenning editors, Springer Verla 2003, 51-54.
- [10] G. B. Gurevich, Foundation of the Theory of Algebraic Invariants, Moscow & Leningrad, GITTL, 1948.
- [11] D. Hilbert, Invariant Theory, Cambridge University Press, 1993.
- [12] Daniele Lazard, Gröbner Bases, Gaussian Elimination and Resolution of Systems of Algebraic Equations in Computer Algebra. UROCAL 1983, J.A Van Hultze lecture notes in Computer science 162. Springer Verlag, New York-Berlin-Heidelberg, 146-156.
- [13] A. M. Liapunov, Problème général de la stabilité du mouvement, J. Math. Studies, Vol. 17, Princeton University Press, 1947.
- [14] C. S. Sibirskii, Introduction to the Algebraic Theory of Invariants of Differential Equations, Nonlinear Science, Theory and Applications, Manchester University Press, 1988.
- [15] J. L. Mott, A. Kandel and T. P. Baker, Discrete Mathematics for Computer Scientists and Mathematicians, Prentice Hall, 1986.

# Periodic and Mean-Periodic Solutions of LODEs with Constant Coefficients

Ivan Dimovski, Margarita Spiridonova  
Institute of Mathematics and Informatics,  
Bulgarian Academy of Sciences  
1113 Sofia, Bulgaria

mspirid@math.bas.bg

## Abstract

A review of our operational calculus approach to obtaining periodic and mean-periodic solutions of LODE with constant coefficients is presented.

Let  $P(\lambda) = a_0\lambda^n + a_1\lambda^{n-1} + \dots + a_{n-1}\lambda + a_n$  be a non-zero polynomial with constant coefficients of degree  $n$  and let us consider an ordinary linear differential equation of the form:

$$P\left(\frac{d}{dt}\right)y = f(t), \quad -\infty < t < \infty \quad (1)$$

Let  $\Phi$  be a linear functional on  $\mathcal{C}(\mathbb{R})$ . We are looking for solutions of (1) which satisfy the relation

$$\Phi \{y(t + \tau)\} = 0 \quad (2)$$

for all  $t \in \mathbb{R}$ , i.e. for mean-periodic solutions of (1) with respect to the functional  $\Phi$ .

A necessary condition for existence of a mean-periodic solution  $y(t)$  of (1) is the requirement the right hand side function  $f(t)$  to be also mean-periodic.

It is shown that the condition (2) may be replaced by a finite number of nonlocal BVCs of the form

$$\Phi \{y^{(k)}\} = 0, \quad k = 0, 1, 2, \dots, \deg P - 1$$

The problem for determining of the periodic and antiperiodic solutions of (1) with period  $T$  is a special kind of this problem.

We develop a Mikusiński type operational calculus (see [1], [2]) based on the non-classical convolution

$$(f * g)(t) = \Phi_\tau \left\{ \int_\tau^t f(t + \tau - \sigma)g(\sigma)d\sigma \right\}. \quad (3)$$

It happens that the  $\Phi$  – mean-periodic functions form an ideal on the convolution algebra  $(\mathcal{C}(\mathbb{R}), *)$ . This fact is used for obtaining of the  $\Phi$  – mean-periodic solutions of (1) in explicit form, both in the non-resonance and in the resonance cases.

A Heaviside type algorithm for obtaining periodic solutions (in the non-resonance and resonance cases) is presented (see [3]). Examples of computation of such solutions in the environment of *Mathematica* system are included. A comparison with other known methods is made.

## References

- [1] Dimovski, I. H. Convolutional Calculus. Kluwer, Dordrecht, 1990.
- [2] Dimovski, I. H. Non-local operational calculi. Proc. Steklov Inst. Math., 1995, Issue 3, 53 – 65.
- [3] Dimovski, I. and M. Spiridonova. Operational Calculus Approach to Nonlocal Cauchy Problems, J. Mathematics in Computer Science, Volume 4, Number 2-3, 2011, 243-258

# Looking for invariant algebraic curves

Antoni Ferragut and Armengol Gasull  
 Universitat Autònoma de Barcelona (Catalonia)

antoni.ferragut@upc.edu

## Abstract

The problem of finding invariant algebraic curves for planar polynomial differential systems  $\dot{x} = P(x, y)$ ,  $\dot{y} = Q(x, y)$  of degree  $d \in \mathbb{N}$  is a classical one. The existence of invariant algebraic curves is a very important matter in the theory of integrability. Darboux related the number of such curves to the existence of a so-called Darboux first integral in the plane. After some years these theorem of Darboux was generalized to count the number of invariant algebraic curves and the number of exponential factors, see [Christpher-Llibre, 2000]. Indeed besides the number of invariant algebraic curves, it is important to count the number of cofactors that we can find. If we have at least  $\binom{d+1}{2}$  of them, then we can construct a Darboux or a Liouville first integral.

Another important fact is that in order to compute the invariant algebraic curves of a polynomial system it is important to know the expression of its cofactor, or to have the maximum of information about it. If we know the expression of the cofactor then to find a solution of equation (1) is (theoretically) easier.

In this work we deal with the problem of finding invariant algebraic curves of polynomial differential systems on the plane and at the same time providing some techniques of simplification of the cofactor that an invariant algebraic curve may have.

It is well-known that an algebraic curve  $f = 0$  is *invariant* for system  $(P, Q)$  if it satisfies the equation

$$Pf_x + Qf_y - kf = 0, \quad (1)$$

for some (complex) polynomial  $k$  of degree at most  $d - 1$ . In [Gasull-Giacomini-Torregrosa, 2007] a method to compute invariant algebraic curves is introduced. This method starts from knowing an analytic solution of the form  $z = y - \alpha(x) = 0$ . If  $f = 0$  is an invariant algebraic curve of degree  $m \in \mathbb{N}$  with cofactor  $k$ , then equation (1) can be written in powers of  $z$ :

$$\sum_{j=0}^{d+m-1} \left( \sum_{i=0}^j [P_{j-i}F'_i + (iQ_{j-i+1} - i\alpha'P_{j-i+1} - K_{j-i})F_i] \right) z^j = 0, \quad (2)$$

where

$$\begin{aligned} f(x, z + \alpha(x)) &= \sum_{i \geq 0} F_i(x)z^i, & k(x, z + \alpha(x)) &= \sum_{i \geq 0} K_i(x)z^i, \\ P(x, z + \alpha(x)) &= \sum_{i \geq 0} P_i(x)z^i, & Q(x, z + \alpha(x)) &= \sum_{i \geq 0} Q_i(x)z^i. \end{aligned}$$

Our approach to this method uses the change of variables  $(x, y) = (u, 1)/v$ , after which we obtain the polynomial system  $\dot{u} = X(u, v)$ ,  $\dot{v} = Y(u, v)$  of degree  $d + 1$ . Now  $v = 0$  is invariant for the new system  $(X, Y)$  and the above method can be applied using this solution (indeed, we have  $\alpha \equiv 0$ ). Equation (2) becomes

$$\sum_{j=0}^{d+m} \left( \sum_{i=0}^j [X_{j-i}F'_i + (iY_{j-i+1} - K_{j-i})F_i] \right) v^j = 0. \quad (3)$$

Hence we need to solve a system of ODE in the variable  $u$ .

It is also important, in the search of invariant algebraic curves, to know the expression of the cofactor as much as possible. We introduce in our work some techniques in order to know whether some coefficients of the cofactor may be always zero, no matter the invariant algebraic curve.

Finally, when dealing with all the ODE in (3) it is important to know under which conditions the solutions of all these ODE are polynomial. We have structured a manner to face

this problem in such a way that we do not need to solve the equations but we can obtain the conditions on the coefficients for having polynomial solutions.

After the explanation of all these new approaches, we provide some examples to which we apply our work. An immediate example of application of all these techniques is to prove that a given polynomial differential system has no algebraic limit cycles.

The approach can be also used to determine whether a polynomial differential system has a rational first integral or not.

### **Keywords**

polynomial vector field, invariant algebraic curve, rational first integral

# Moving Frames and Noether's Conservation Laws – the General Case

Tânia M. N. Gonçalves  
Universidade Federal de São Carlos (Brazil)

Elizabeth L. Mansfield  
University of Kent (United Kingdom)

`tmng@kentforlife.net`

## Abstract

In recent works, the authors have considered Lagrangians invariant under a Lie group action, in the case where the Lagrangian may be parametrized so that the independent variables are each invariant under the action. We were able to calculate the Euler-Lagrange equations for the invariants in terms of the standard Euler operator and a ‘syzygy’ operator specific to the action and which is readily calculated. Further, we were able to obtain the linear space of conservation laws in terms of vectors of invariants and the adjoint representation of a moving frame for the Lie group action. This allowed us to simplify the calculation for the extremals in the original variables, once the Euler-Lagrange equations for the invariants were solved, for all three  $SL(2)$  and the standard  $SE(3)$  actions.

In this talk, we show how our ideas may be extended to cases where reparametrization of the independent variables is difficult, impossible, or undesired. We take for our main expository example the standard linear action of  $SL(2)$  on the two independent variables. This choice is motivated by applications to variational fluid problems which conserve potential vorticity. We note that Kogan and Olver previously handled the one-dimensional case using a variational tricomplex.

## Keywords

Variational problems, Invariant calculus of variations, Noether's conservation laws, Moving frames

# Interpolation with integral and Stieltjes conditions

Anja Korporal, Georg Regensburger

Johann Radon Institute for Computational and Applied Mathematics (RICAM)  
Linz, Austria

`anja.korporal@oeaw.ac.at`

## **Abstract**

From Hermite interpolation, we know that there exists a unique polynomial of minimal degree taking prescribed values and derivatives at finitely many points. In the context of linear ordinary boundary problems and integro-differential operators, also more general linear conditions appear naturally. These so-called Stieltjes boundary conditions are linear combinations of point evaluations of derivatives (local conditions) and definite integrals with weight functions (global conditions). In this talk, we study related interpolation problems. We show in particular that for integral conditions with monomial weight functions together with Hermite conditions with two evaluation points there exists a unique interpolating polynomial of minimal degree. We discuss ongoing work on various generalizations and also applications to singular boundary problems.

## **Keywords**

Interpolation, Integral Conditions, Stieltjes Conditions, Singular Boundary Problems



# On Completely Integrable Pfaffian Systems with Normal Crossings

Sumayya Suzy Maddah  
 University of Limoges (France)  
 sumayya-suzy.maddah@etu.unilim.fr

## Abstract

Let  $\mathbb{C}$  be the field of complex numbers. We denote by  $\mathcal{O}$  the ring  $\mathbb{C}[[x_1, \dots, x_m]]$  of formal power series in  $x = (x_1, \dots, x_m)$  over  $\mathbb{C}$ . In this talk we consider the class of the so-called *completely integrable Pfaffian systems with normal crossings*, that is, the class of linear systems of partial differential equations in  $m$  variables and dimension  $n$  of the form

$$\begin{cases} x_1^{p_1+1} \frac{\partial Y}{\partial x_1} = A^{(1)}(x)Y \\ \vdots \\ x_m^{p_m+1} \frac{\partial Y}{\partial x_m} = A^{(m)}(x)Y \end{cases}$$

where  $A^{(1)}, \dots, A^{(m)}$  are matrices with entries in  $\mathcal{O}$  satisfying the integrability conditions

$$x_i^{p_i+1} \frac{\partial A^{(j)}}{\partial x_i} + A^{(j)} A^{(i)} = x_j^{p_j+1} \frac{\partial A^{(i)}}{\partial x_j} + A^{(i)} A^{(j)}.$$

The  $m$ -tuple  $(p_1, \dots, p_m)$  of nonnegative integers is called the Poincaré rank of the system. Pfaffian systems arise in the studies of aerospace and celestial mechanics (see, e.g., [8]) and by far the most important for applications are those with normal crossings (see, e.g., [11]). The theoretical results from [9, 10] show that a fundamental matrix of formal solutions can be written as

$$\Phi(x_1^{1/s_1}, \dots, x_m^{1/s_m}) \prod_{i=1}^m x_i^{\Lambda_i} \prod_{i=1}^m \exp(Q_i(x_i^{-1/s_i})) \quad (1)$$

where for  $1 \leq i \leq m$ ,  $s_i$  is a nonzero natural integer and

- $\Phi$  is an invertible meromorphic series in  $(x_1^{1/s_1}, \dots, x_m^{1/s_m})$  over  $\mathbb{C}$ ;
- $Q_i$  is a diagonal matrix containing polynomials in  $x_i^{-1/s_i}$  over  $\mathbb{C}$  without constant terms, called *exponential polynomial matrix*;
- $\Lambda_i$  is a constant matrix commuting with  $Q_i$ .

However, the formal reduction, i.e. the algorithmic procedure that computes the transformation which takes the system into its canonical form so that formal solutions can be constructed, is a question of another nature.

The particular case, when  $m = 1$ , is the case of system of ordinary differential equations which have been studied extensively (see, e.g., [2, 13] and references therein). Moreover, unlike the case of  $m > 1$ , algorithms to related problems leading to the construction of the formal solutions have been developed by various authors (see, e.g., [1, 3, 7, 12] and references therein). The package ISOLDE [6] written in the computer algebra system Maple is dedicated to the symbolic resolution of systems of ordinary linear differential equations and more generally linear functional matrix equations.

For  $m = 2$ , a first step in formal reduction was set up in [4] where the problem of *rank reduction* was tackled. As a second step, we give here an explicit method to compute the *exponential polynomial matrices* in the case of two variables. Upon changes of exponential, our work reduces formal reduction to the task of constructing a basis of the  $\mathbb{C}$ -space of *regular* solutions (see, e.g., [5]). Moreover, it gives information on the formal invariants of the system.

## Keywords

Linear Systems of Partial Differential Equations, Formal Solutions, Singular Points

This work is a part of my Ph. D. thesis which is in progress and jointly supervised by Pr. Moulay Barkatou at the University of Limoges and Dr. Hassan Abbas at the Lebanese University.

## References

- [1] H. Abbas. Contribution à l'étude de la reduction formelle des systèmes meromorphes Linéaires. PhD Thesis. *Institute Nationale Polytechnique de Grenoble*, France, 1993.
- [2] W. Balser. Formal Power Series and Linear Systems of Meromorphic Ordinary Differential Equations. *Springer-Verlag*, New York, 2000.
- [3] M. Barkatou. An algorithm to compute the exponential part of a formal fundamental matrix solution of a linear differential system. *Journal of App. Alg. in Eng. Comm. and Comp.*, 8(1):1-23, 1997.
- [4] M. Barkatou and N. Le Roux. Rank Reduction of a class of Pfaffian Systems in Two Variables. In *J.G. Dumas*. Editor : ISSAC 2006, pages 204-211, ACM Press, 2006.
- [5] M. Barkatou and E. Pflugel. An algorithm computing the regular formal formal solutions of a system of linear differential equations. *Journal of Sym. Comput.*, 28, 569-587, 1999.
- [6] M. Barkatou and E. Pflugel. ISOLDE, Integration of Systems of Ordinary Linear Differential Equations. Available at: <http://isolde.sourceforge.net/>
- [7] M. Barkatou and E. Pflugel. On the Moser-and super-reduction algorithms of systems of linear differential equations and their complexity. *Journal of Sym. Comput.*, 44 (8), 1017-1036, 2009.
- [8] R. Broucke. On Pfaff's equations of motion in dynamics; Applications to Satellite Theory. *Journal of Celestial Mechanics*, 18(3): 207-222, 1978.
- [9] H. Charrière. Triangulation Formelle de certains Systèmes de Pfaff Complètement Intégrables et Application à l'étude  $C^\infty$  des Systèmes non Linéaires. *Ann. Scuola Norm. Sup. Pisa CI. Sci.*, 7(4): 625 - 714, 1980.
- [10] A. van den Essen et A.H.M. Levelt. Irregular Singularities in Several Variables. *Memoirs of AMS*, 40(270), 1982.
- [11] D. Novikov, S. Yakovenko. Lectures on meromorphic flat connections. Available at: [arXiv:math/0212334](http://arXiv:math/0212334)
- [12] E. Pflugel. Effective Formal Reduction of Linear Differential Systems. *Journal of App. Alg. in Eng. Comm. and Comp.*, 10, 153-187, 2000.
- [13] W. Wasow. Asymptotic Expansions for Ordinary Differential Equations. *Dover Phoenix Editions*, 2002.

# Linear Boundary Problems for Partial Differential Equations: Algebraic Setup and First Steps for Constant Coefficients

Nalina Phisanbut, Markus Rosenkranz\*  
University of Kent (United Kingdom)

`N.Phisanbut@kent.ac.uk`

## Abstract

We propose an algebraic framework for studying linear boundary problems for partial differential equations. Our long-term plan is to apply this framework to linear differential equations with constant coefficients, going through the following three stages:

1. The Cauchy problem for completely reducible operators.
2. The Cauchy problem for hyperbolic equations.
3. More general boundary problems for equations of various type.

In this talk we concentrate on (1), outline an algebraic strategy for (2), and round up with some rough ideas towards (3).

## Keywords

Linear partial differential equations, boundary problems, Green's operators, integro-differential algebras, integro-differential operators.

---

\*The authors acknowledge support from the EPSRC First Grant EP/I037474/1.

# On the arithmetic of d'Alembertian functions

Clemens G. Raab  
Deutsches Elektronen-Synchrotron, Zeuthen (Germany)

`clemens.raab@desy.de`

## **Abstract**

D'Alembertian functions can be characterized as nested indefinite integrals over hyperexponential functions. The representation of d'Alembertian functions in terms of such nested integrals is far from unique. We define a family of basis functions by restricting the hyperexponential functions occurring in the integrands. Based on this we obtain a canonical form for d'Alembertian functions. We also exhibit the algebraic relations among d'Alembertian functions. An algorithm for computing canonical forms of d'Alembertian functions and their indefinite integrals will be given, which builds on corresponding results for hyperexponential functions.

## **Keywords**

D'Alembertian functions, Hyperexponential functions, Nested integrals, Canonical forms

# Applying Thomas decomposition and algebraic analysis to certain nonlinear PDE systems

Daniel Robertz  
Lehrstuhl B für Mathematik  
RWTH Aachen University (Germany)

`daniel@momo.math.rwth-aachen.de`

## **Abstract**

This talk is about work in progress in collaboration with Thomas Cluzeau, Université de Limoges, and Alban Quadrat, Inria Saclay. We report on first steps of a study of certain systems of nonlinear partial differential equations using a new algebraic analysis approach. By applying module-theoretic techniques to a new kind of linearization of the given equations, e.g., conservation laws of the given nonlinear system are computed. This approach relies on methods of symbolic computation for both nonlinear and linear differential equations: a preparatory step applies a decomposition technique as proposed by J. M. Thomas in the 1930s; the linearized system is dealt with using a version of Janet's algorithm performing normal form computations for the symbolic coefficients of the linearization modulo the nonlinear system.

## **Keywords**

Nonlinear partial differential equations, conservation laws, Thomas decomposition,  
Janet bases, linearization, algebraic analysis

# Sparse differential resultant formulas: between the linear and the nonlinear case

Sonia L. Rueda

E.T.S. Arquitectura, Universidad Politécnica de Madrid (Spain)

`sonialuisa.rueda@upm.es`

## Abstract

A matrix representation of the sparse differential resultant is the basis for efficient computation algorithms, whose study promises a great contribution to the development and applicability of differential elimination techniques. It is shown how sparse linear differential resultant formulas provide bounds for the order of derivation, even in the nonlinear case, and they also provide (in many cases) the bridge with results in the nonlinear algebraic case.

## Keywords

Differential resultant, sparse differential polynomial, super essential, algebraically essential

## 1 Introduction

Differential elimination is an important operation in differential algebraic geometry that, in theory, can be achieved through Gröbner bases, characteristic sets and differential resultants. For applications, sparse differential elimination is the operation that is naturally necessary. Sparse algebraic resultants have been broadly studied, regarding theory and computation (see [2], [3], [8] and references there in), meanwhile differential resultants were recently defined in [4] for sparse Laurent differential polynomials.

The computation and applicability of sparse algebraic resultants attained great benefits from having close formulas for their representation. Similar formulas in the differential case would improve the existing bounds for degree and order of the sparse differential resultant and therefore the existing algorithms for its computation. Matrix formulas would also contribute to the development of methods to predict the support of the sparse differential resultant, achieving similar benefits to the ones obtained in the algebraic case. In the differential case, these so called Macaulay style formulas do not exist. The differential resultant formula defined by Carrà-Ferro in [1], is the algebraic resultant of Macaulay, of a set of derivatives of the ordinary differential polynomials in  $\mathfrak{P}$ . Already in the linear sparse generic case, these formulas vanish often, giving no information about the differential resultant  $\partial\text{Res}(\mathfrak{P})$ , and this was the starting point of my interest in this topic ([5], [6]).

In [7], determinantal formulas are provided for systems of  $n$  linear nonhomogeneous (non necessarily generic) differential polynomials  $\mathcal{P}$  in a set  $U$  of  $n - 1$  differential indeterminates. These formulas are determinants of coefficient matrices of appropriate sets of derivatives of the differential polynomials in  $\mathcal{P}$ , or in a linear perturbation  $\mathcal{P}_\epsilon$  of  $\mathcal{P}$ , and allow the elimination of the differential variables in  $U$  from  $\mathcal{P}$ . In particular, the formula  $\partial\text{FRes}(\mathcal{P})$  is the determinant of a matrix  $\mathcal{M}(\mathcal{P})$  having no zero columns if the system  $\mathcal{P}$  is “super essential”. As an application, if the system  $\mathfrak{P}$  is sparse generic, such formulas can be used to compute the differential resultant  $\partial\text{Res}(\mathfrak{P})$  introduced in [4].

To approach the nonlinear case, one should observe that differential polynomials can be sparse in degree and in order of derivation. One can start with the problem of taking the appropriate set of derivatives of the elements in  $\mathcal{P}$  to get a system of differential polynomials  $\text{ps}(\mathcal{P})$ , that seen as algebraic, should have  $L$  polynomials in  $L - 1$  variables. For this purpose, we extend here the “super essential” condition to non linear polynomials, taking into consideration the sparsity in the order. Results obtained in the linear case can also be used to check, in some cases, the existence

of the algebraic resultant of the generic system of algebraic polynomials whose specialization is  $\text{ps}(\mathcal{P})$ , providing a link with the machinery available in the sparse algebraic case.

## 2 Sparse differential resultant

Let  $\mathbb{D}$  be an ordinary differential domain with derivation  $\partial$ . Let  $U = \{u_1, \dots, u_{n-1}\}$  be a set of differential indeterminates over  $\mathbb{D}$ . By  $\mathbb{N}$  we mean the natural numbers including 0. For  $k \in \mathbb{N}$ , we denote by  $u_{j,k}$  the  $k$ -th derivative of  $u_j$  and for  $u_{j,0}$  we simply write  $u_j$ . We denote by  $\{U\}$  the set of derivatives of the elements of  $U$ ,  $\{U\} = \{\partial^k u \mid u \in U, k \in \mathbb{N}\}$ , and by  $\mathbb{D}\{U\}$  the ring of differential polynomials in the differential indeterminates  $U$ , which is a differential ring with derivation  $\partial$ . Given a subset  $\mathcal{U} \subset \{U\}$ , we denote by  $\mathbb{D}[\mathcal{U}]$  the ring of polynomials in the indeterminates  $\mathcal{U}$ . Given  $f \in \mathbb{D}\{U\}$  and  $y \in U$ , we denote by  $\text{ord}(f, y)$  the order of  $f$  in the variable  $y$ . If  $f$  does not have a term in  $y$  then we define  $\text{ord}(f, y) = -1$ . The order of  $f$  equals  $\max\{\text{ord}(f, y) \mid y \in U\}$ .

Let  $\mathcal{P} := \{f_1, \dots, f_n\}$  be a system of differential polynomials in  $\mathbb{D}\{U\}$ . We assume that:

(P1) The order of  $f_i$  is  $o_i \geq 0$ ,  $i = 1, \dots, n$ . So that no  $f_i$  belongs to  $\mathbb{D}$ .

(P2)  $\mathcal{P}$  contains  $n$  distinct polynomials.

(P3)  $\mathcal{P}$  is a nonhomogeneous system. At least one of the polynomials in  $\mathcal{P}$  has nonzero degree zero term.

Let  $[\mathcal{P}]$  denote the differential ideal generated by  $\mathcal{P}$  in  $\mathbb{D}\{U\}$ . Our goal is to obtain elements of differential elimination ideal  $[\mathcal{P}] \cap \mathbb{D}$ , using differential resultant formulas.

Let us consider a generic system of nonhomogeneous sparse differential polynomials

$$\mathfrak{P} = \left\{ \mathbb{F}_i := c_i + \sum_{h=1}^{m_i} c_{i,h} M_{i,h} \mid i = 1, \dots, n \right\},$$

$c_i$  and  $c_{i,h}$  are differential indeterminates over  $\mathbb{Q}$ ,  $m_i$  is the number of monomials of  $\mathbb{F}_i$ , and  $M_{i,h}$  are monomials in the variables  $\{U\}$ . Let us consider the differential field  $\mathbb{K} = \mathbb{Q}\langle c_{i,h} \mid i=1, \dots, n, h=1, \dots, m_i \rangle$  and observe that  $\mathfrak{P}$  is a system in  $\mathbb{D}\{U\}$ , with  $\mathbb{D} = \mathbb{K}\{c_1, \dots, c_n\}$ . If the differential elimination ideal  $[\mathfrak{P}] \cap \mathbb{D}$  has dimension  $n - 1$  then  $[\mathfrak{P}] \cap \mathbb{D} = \text{sat}(\partial \text{Res}(\mathfrak{P}))$ , the saturated ideal determined by a differential polynomial  $\partial \text{Res}(\mathfrak{P})$ , which is called the **sparse differential resultant** of  $\mathfrak{P}$ . Sparse differential resultants were defined in [4], were their existence is proved to be equivalent with the differentially essential condition on  $\mathfrak{P}$ .

## 3 A system $\text{ps}(\mathcal{P})$ of $L$ polynomials in $L-1$ algebraic variables

Given  $f \in \mathbb{D}\{U\}$ , let us denote the differential support in  $u_j$  of  $f$  by

$$\mathfrak{S}_j(f) = \{k \in \mathbb{N} \mid u_{j,k}/M \text{ for some monomial } M \text{ of } f\}.$$

Note that  $\text{ord}(f, u_j) := \max \mathfrak{S}_j(f)$  and define  $\text{lord}(f, u_j) := \min \mathfrak{S}_j(f)$ . For  $j = 1, \dots, n-1$ , we define the next positive integers, to construct convenient intervals bounding the differential support sets  $\mathfrak{S}_j(f_i)$ ,

$$\begin{aligned} \bar{\gamma}_j(\mathcal{P}) &:= \min\{o_i - \text{ord}(f_i, u_j) \mid \mathfrak{S}_j(f_i) \neq \emptyset, i = 1, \dots, n\}, \\ \underline{\gamma}_j(\mathcal{P}) &:= \min\{\text{lord}(f_i, u_j) \mid \mathfrak{S}_j(f_i) \neq \emptyset, i = 1, \dots, n\}, \end{aligned} \quad (1)$$

Given  $j \in \{1, \dots, n-1\}$ , observe that, for all  $i$  such that  $\mathfrak{S}_j(f_i) \neq \emptyset$  we have

$$\mathfrak{S}_j(f_i) \subseteq [\underline{\gamma}_j(\mathcal{P}), o_i - \bar{\gamma}_j(\mathcal{P})]. \quad (2)$$

Finally,  $\gamma(\mathcal{P}) := \sum_{j=1}^{n-1} \gamma_j(\mathcal{P})$ , with  $\gamma_j(\mathcal{P}) := \underline{\gamma}_j(\mathcal{P}) + \bar{\gamma}_j(\mathcal{P})$ .

Let  $N := \sum_{i=1}^n o_i$ . If  $N - o_i - \gamma(\mathcal{P}) \geq 0$ ,  $i = 1, \dots, n$ , the sets of lattice points  $\mathbb{I}_i := [0, N - o_i - \gamma(\mathcal{P})] \cap \mathbb{N}$  are non empty. We define the set of differential polynomials

$$\text{ps}(\mathcal{P}) := \{\partial^k f_i \mid k \in \mathbb{I}_i, i = 1, \dots, n\}, \quad (3)$$

containing  $L := \sum_{i=1}^n (N - o_i - \gamma(\mathcal{P}) + 1)$  differential polynomials, whose variables belong to the set  $\mathcal{V}$  of  $L - 1$  differential indeterminates

$$\mathcal{V} := \{u_{j,k} \mid k \in [\underline{\gamma}_j(\mathcal{P}), N - \bar{\gamma}_j(\mathcal{P}) - \gamma(\mathcal{P})] \cap \mathbb{N}, j = 1, \dots, n - 1\}.$$

In general, given  $j \in \{1, \dots, n - 1\}$  we have

$$\cup_{f \in \text{ps}(\mathcal{P})} \mathfrak{S}_j(f) \subseteq [\underline{\gamma}_j(\mathcal{P}), N - \bar{\gamma}_j(\mathcal{P}) - \gamma(\mathcal{P})] \cap \mathbb{N}, \quad (4)$$

and we cannot guarantee that the equality holds. If there exists  $j$  such that (4) is not an equality, we will say that the system  $\mathcal{P}$  is **sparse in the order**.

Let  $x_{i,j}$ ,  $i = 1, \dots, n$ ,  $j = 1, \dots, n - 1$  be algebraic indeterminates over  $\mathbb{Q}$ , the field of rational numbers. Let  $X(\mathcal{P}) = (X_{i,j})$  be the  $n \times (n - 1)$  matrix, such that

$$X_{i,j} := \begin{cases} x_{i,j}, & \mathfrak{S}_j(f_i) \neq \emptyset, \\ 0, & \mathfrak{S}_j(f_i) = \emptyset. \end{cases} \quad (5)$$

We denote by  $X_i(\mathcal{P})$ ,  $i = 1, \dots, n$ , the submatrix of  $X(\mathcal{P})$  obtained by removing its  $i$ th row. Thus  $X(\mathcal{P})$  is an  $n \times (n - 1)$  matrix with entries in the field  $\mathbb{K} := \mathbb{Q}(X_{i,j} \mid X_{i,j} \neq 0)$ .

The notion of super essential system of differential polynomials was introduced in [7], for systems of linear differential polynomials and it is extended here to the nonlinear case.

**Definition 3.1** *The system  $\mathcal{P}$  is called super essential if  $\det(X_i(\mathcal{P})) \neq 0$ ,  $i = 1, \dots, n$ .*

Given a super essential system  $\mathcal{P}$  (non necessarily linear), it can be proved as in [7], Lemma 3.6 that  $N - o_i - \gamma(\mathcal{P}) \geq 0$ ,  $i = 1, \dots, n$ . Furthermore, the next result can be shown adapting the proof of [7], Theorem 3.11 to the nonlinear case.

**Theorem 3.2** *If  $\mathcal{P}$  is super essential then*

$$\cup_{f \in \text{ps}(\mathcal{P})} \mathfrak{S}_j(f) = [\underline{\gamma}_j(\mathcal{P}), N - \bar{\gamma}_j(\mathcal{P}) - \gamma(\mathcal{P})] \cap \mathbb{N}, \quad j = 1, \dots, n - 1.$$

*That is,  $\mathcal{P}$  is a system of  $L$  polynomials in  $L - 1$  algebraic indeterminates.*

It can be proved as in [7], Section 4 that every system  $\mathcal{P}$  contains a super essential subsystem  $\mathcal{P}^*$  and if  $\text{rank}(X(\mathcal{P})) = n - 1$  then  $\mathcal{P}^*$  is unique.

**Example 3.3** *Let us consider the systems  $\mathcal{P}_1 = \{f_1, f_2, f_3, f_4\}$  and  $\mathcal{P}_2 = \{f_1, f_2, f_3, f_5\}$  with*

$$f_1 = 2 + u_1 u_{1,1} + u_{1,2}, f_2 = u_1 u_{1,2}, f_3 = u_2 u_{3,1}, f_4 = u_{1,1} u_2, f_5 = u_{1,2},$$

$$X(\mathcal{P}_1) = \begin{pmatrix} x_{1,1} & 0 & 0 \\ x_{2,1} & 0 & 0 \\ 0 & x_{3,2} & x_{3,3} \\ x_{4,1} & x_{4,2} & 0 \end{pmatrix} \text{ and } X(\mathcal{P}_2) = \begin{pmatrix} x_{1,1} & 0 & 0 \\ x_{2,1} & 0 & 0 \\ 0 & x_{3,2} & x_{3,3} \\ x_{4,1} & 0 & 0 \end{pmatrix}.$$

$\mathcal{P}_1$  is not super essential but since  $\text{rank}(X(\mathcal{P}_1)) = 3$ , it has a unique super essential subsystem, which is  $\{f_1, f_2\}$ .  $\mathcal{P}_2$  is not super essential and  $\text{rank}(X(\mathcal{P}_2)) < 3$ , super essential subsystems are  $\{f_1, f_2\}$ ,  $\{f_1, f_3\}$  and  $\{f_2, f_3\}$ .

## 4 Associated sparse algebraic resultant

We can establish a bijection between  $\mathcal{V}$  and the set  $Y = \{y_1, \dots, y_{L-1}\}$  of  $L - 1$  algebraic indeterminates. This can be extended to a ring homomorphism  $\beta : \mathbb{D}[\mathcal{V}] \rightarrow \mathbb{D}[Y]$ . Monomials in  $\mathbb{D}[Y]$  are  $Y^\alpha = y_1^{\alpha_1} \dots y_{L-1}^{\alpha_{L-1}}$  with  $\alpha = (\alpha_1, \dots, \alpha_{L-1}) \in \mathbb{N}^{L-1}$ . Given  $f \in \mathbb{D}[\mathcal{V}]$ , we denote the algebraic support  $\mathcal{A}(f)$  of  $f$ , with  $\beta(f) = \sum_{\alpha \in \mathbb{N}^{L-1}} a_\alpha Y^\alpha$ , as  $\mathcal{A}(f) := \{\alpha \in \mathbb{N}^{L-1} \mid a_\alpha \neq 0\}$ .

We define the algebraic system of generic polynomials associated to  $\mathcal{P}$  as

$$\text{ags}(\mathcal{P}) = \left\{ \sum_{\alpha \in \mathcal{A}(f)} c_\alpha(f) Y^\alpha \mid f \in \text{ps}(\mathcal{P}) \right\},$$



where  $c_\alpha(f)$  are algebraic indeterminates over  $\mathbb{Q}$ . Let us denote  $c(f) := c_{\bar{0}}(f)$ ,  $f \in \text{ps}(\mathcal{P})$ , where  $\bar{0}$  is the zero of  $\mathbb{N}^{L-1}$ .

Given a subsystem  $\mathcal{S} \subseteq \text{ags}(\mathcal{P})$ , let us define the fields

$$\mathcal{E} := \mathbb{Q}(c_\alpha(f) \mid f \in \text{ps}(\mathcal{P}), \alpha \in \mathcal{A}(f) \setminus \{\bar{0}\}), \quad \mathcal{E}_{\mathcal{S}} := \mathcal{E}(f - c(f) \mid f \in \mathcal{S}).$$

As in [4], a subsystem of polynomials  $\mathcal{S}$  of  $\text{ags}(\mathcal{P})$  is said to be **algebraically independent** if the transcendence degree, of  $\mathcal{E}_{\mathcal{S}}$  over  $\mathcal{E}$ ,  $\text{trdeg}(\mathcal{E}_{\mathcal{S}}/\mathcal{E}) = |\mathcal{S}|$ , otherwise it is said to be **algebraically dependent**. A subsystem of polynomials  $\mathcal{S}$  of  $\text{ags}(\mathcal{P})$  is said to be **algebraically essential** if  $\mathcal{S}$  is algebraically dependent and every proper subsystem  $\mathcal{S}'$  of  $\mathcal{S}$  is algebraically independent.

Assuming that  $\cup_{f \in \text{ps}(\mathcal{P})} \mathcal{A}(f) \setminus \{\bar{0}\}$  spans  $\mathbb{Z}^{L-1}$ , it was proved in [8] that, a necessary and sufficient condition for the existence of the algebraic resultant  $R$  of  $\text{ags}(\mathcal{P})$  is the existence of a unique algebraically essential subsystem of  $\text{ags}(\mathcal{P})$ .

**Example 4.1** *Let us consider the system  $\mathcal{P} = \{f_1, f_2\}$  in  $\mathbb{D}\{u\}$ ,*

$$\begin{aligned} f_1 &= a_2x + (a_1 + a_4x)u + u' + (a_3 + a_6x)u^2 + a_5u^3, \\ f_2 &= x' + (b_1 + b_3x)u + (b_2 + b_5x)u^2 + b_4u^3, \end{aligned}$$

with  $a_i, b_j$  algebraic indeterminates over  $\mathbb{Q}$ ,  $\mathbb{D} = \mathbb{Q}(t)[a_i, b_j]\{x\}$  and  $\partial = \frac{\partial}{\partial t}$ . Since  $\text{ps}(\mathcal{P}) = \{f_1, f_2, \partial f_2\}$ , with  $\partial f_2 = x'' + b_3x'u + (b_3x + b_1)u' + b_5x'u^2 + (2b_5x + 2b_2)uu' + 3b_4u^2u'$  and  $\mathcal{V} = \{u, u'\}$ , we have the following system of algebraic generic polynomials in  $y_1, y_2$

$$\text{ags}(\mathcal{P}) = \left\{ \begin{array}{l} P_1 = c_{(0,0)}^1 + c_{(1,0)}^1 y_1 + c_{(0,1)}^1 y_2 + c_{(2,0)}^1 y_1^2 + c_{(3,0)}^1 y_1^3, \\ P_2 = c_{(0,0)}^2 + c_{(1,0)}^2 y_1 + c_{(2,0)}^2 y_1^2 + c_{(3,0)}^2 y_1^3, \\ P_3 = c_{(0,0)}^3 + c_{(1,0)}^3 y_1 + c_{(0,1)}^3 y_2 + c_{(2,0)}^3 y_1^2 + c_{(1,1)}^3 y_1 y_2 + c_{(2,1)}^3 y_1^2 y_2 \end{array} \right\},$$

where  $c_{\alpha, f_1}$ ,  $c_{\alpha, f_2}$  and  $c_{\alpha, \partial f_2}$  are denoted by  $c_\alpha^1$ ,  $c_\alpha^2$  and  $c_\alpha^3$  respectively,  $\alpha \in \mathbb{N}^2$ . Observe that  $\text{ags}(\mathcal{P})$  is algebraically essential because the linear part of the polynomials in  $\text{ags}(\mathcal{P})$ ,  $\{c_{(0,0)}^1 + c_{(1,0)}^1 y_1 + c_{(0,1)}^1 y_2, c_{(0,0)}^2 + c_{(1,0)}^2 y_1, c_{(0,0)}^3 + c_{(1,0)}^3 y_1 + c_{(0,1)}^3 y_2\}$  is an algebraically essential system. Thus the algebraic resultant  $R$  of  $\text{ags}(\mathcal{P})$  exists and it generates the algebraic ideal  $(\text{ags}(\mathcal{P})) \cap \mathbb{Q}[c_\alpha^i \mid \alpha \in \mathcal{A}(f_i), i = 1, 2, \alpha \in \mathcal{A}(\partial f_2), i = 3] = (R)$ . Using "toricres04", Maple 9 code for sparse (toric) resultant matrices by I.Z. Emiris, [2], we obtain a matrix  $M$  whose determinant is  $c_{(0,0)}^3 R$ . This matrix is the coefficient matrix of the polynomials

$$y_1 P_1, y_1 y_2 P_1, y_1 y_2^2 P_1, y_1^2 P_2, y_1 y_2 P_2, y_1^2 y_2 P_2, y_1 y_2^2 P_2, y_1^2 y_2^2 P_2, y_1 P_3, y_1 y_2 P_3, y_1 y_2^2 P_3, y_1 y_2^3 P_3$$

in the monomials  $y_1, y_1^2, y_1 y_2, y_1^2 y_2, y_1 y_2^2, y_1^2 y_2^2, y_1 y_2^3, y_1^2 y_2^3, y_1 y_2^4, y_1^2 y_2^4, y_1 y_2^5, y_1^2 y_2^5$ . The specialization of the algebraic indeterminates  $\{c_\alpha^i \mid \alpha \in \mathcal{A}(f_i), i = 1, 2, \alpha \in \mathcal{A}(\partial f_2), i = 3\}$  in  $R$ , to the corresponding coefficients of  $\text{ps}(\mathcal{P})$ , gives a nonzero differential polynomial  $\bar{R}$  in the differential elimination ideal  $[\mathcal{P}] \cap \mathbb{D}$ .

## 5 Some consequences from results in the linear case

Given a linear system  $\mathcal{P}$ , differential resultant formulas were defined in [7], see also [5] and [6]. In particular, if  $N - o_i - \gamma \geq 0$ ,  $i = 1, \dots, n$ , the formula  $\partial \text{FRes}(\mathcal{P})$  is the determinant of the  $L \times L$  coefficient matrix  $\mathcal{M}(\mathcal{P})$  of the set of polynomials  $\text{ps}(\mathcal{P})$  in the set of variables  $\mathcal{V}$ . Furthermore, if  $\mathcal{P}$  is super essential, by Theorem 3.2 (which is [7], Theorem 3.11 in the linear case), the matrix  $\mathcal{M}(\mathcal{P})$  has no zero columns.

Let  $\mathcal{P}$  be a linear system and let  $\mathcal{S} = \text{ags}(\mathcal{P})$ , which is also a linear system. For every subsystem  $\mathcal{S}'$  of  $\mathcal{S}$ , let  $C(\mathcal{S}')$  be the coefficient matrix of the homogeneous part of the polynomials in  $\mathcal{S}'$  in the variables  $Y$ , this is a  $|\mathcal{S}'| \times L - 1$  matrix. Adapting the results in [7], Section 4 the next proposition is proved.

**Proposition 5.1** *Let  $\mathcal{P}$  be a super essential linear system and let  $\mathcal{S} = \text{ags}(\mathcal{P})$ . The following statements hold:*

1. *Let  $\mathcal{S}_l$  be the subsystem of  $\mathcal{S}$  obtained by removing its  $l$ th polynomial,  $l = 1, \dots, L$ .  $\mathcal{S}$  is algebraically essential if and only if  $\det(C(\mathcal{S}_l)) \neq 0$ ,  $l = 1, \dots, L$ .*

2. *There exists an algebraically essential subsystem of  $\mathcal{S}$ .*
3.  *$\text{rank}(C(\mathcal{S})) = |\mathcal{S}| - 1 = L - 1$  if and only if there exists a unique algebraically essential subsystem  $\mathcal{S}^*$  of  $\mathcal{S}$ .*

Let  $\mathfrak{P}$  be a generic system of sparse linear differential polynomials. As a consequence of the previous result, if  $\partial\text{FRes}(\mathfrak{P}) \neq 0$  then  $\text{ags}(\mathfrak{P})$  contains a unique algebraically essential subsystem  $\mathcal{S}^*$ , which corresponds to a subsystem of  $\text{ps}(\mathfrak{P})$  that we call  $S^*$ . Let  $\mathcal{M}(S^*)$  be the coefficient matrix of  $S^*$ , which is  $|S^*| \times |S^*|$ . The rows and columns of  $\mathcal{M}(\mathfrak{P})$  can be reorganized to obtain a matrix

$$\begin{bmatrix} E & * \\ 0 & \mathcal{M}(S^*) \end{bmatrix}, \text{ such that } \partial\text{FRes}(\mathfrak{P}) = \pm \det(E) \det(\mathcal{M}(S^*)), \text{ and } \partial\text{Res}(\mathfrak{P}) = \det(\mathcal{M}(S^*)).$$

Using the previous results, a family of systems  $\mathcal{F}$  of generic sparse differential polynomials can be obtained, so that degree bounds of the sparse differential resultant can be given in terms of mixed volumes. In [4], such bound was given for the case of generic non sparse differential polynomials. Let  $\text{lin}(\mathfrak{P})$  be the system of the linear parts of the polynomials in  $\mathfrak{P}$ . We define  $\mathcal{F}$  as the family of all systems of generic sparse differential polynomials in the variables  $\{U\}$  such that the supports of the polynomials in  $\text{ps}(\text{lin}(\mathfrak{P}))$  jointly span  $\mathbb{Z}^{L-1}$  and  $\partial\text{FRes}(\text{lin}(\mathfrak{P})) \neq 0$ , see Example 4.1. For every  $\mathfrak{P}$  in  $\mathcal{F}$ ,  $\text{ags}(\text{lin}(\mathfrak{P}))$  is algebraically essential and furthermore  $\text{ags}(\mathfrak{P})$  is algebraically essential, thus the algebraic resultant of  $\text{ags}(\mathfrak{P})$  exists and it can be used to give bounds of the degrees in terms of mixed volumes.

**Acknowledgments:** This work was developed, and partially supported, under the research project MTM2011-25816-C02-01. The author belongs to the Research Group ASYNACS (Ref. CCEE2011/R34).

## References

- [1] Carrà-Ferro, G., 1997. A resultant theory for ordinary algebraic differential equations. Lecture Notes in Computer Science, 1255. Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. Proceedings.
- [2] Canny, J.F. and Emiris, I.Z., 2000. A Subdivision-Based Algorithm for the Sparse Resultant, J. ACM 47,417-451.
- [3] D'Andrea, C., 2002. Macaulay Style Formulas for Sparse Resultants. Trans. of AMS, 354(7), 2595-2629.
- [4] Li, W., Yuan, C.M., Gao, X.S., 2012. Sparse Differential Resultant for Laurent Differential polynomials. In arXiv:1111.1084v3, 1-70.
- [5] Rueda, S.L. and Sendra, J.F., 2010. Linear complete differential resultants and the implicitization of linear DPPEs. Journal of Symbolic Computation, 45, 324-341.
- [6] Rueda, S.L., 2011. A perturbed differential resultant based implicitization algorithm for linear DPPEs. Journal of Symbolic Computation, 46, 977-996.
- [7] Rueda, S.L., 2013. Linear sparse differential resultant formulas. Linear Algebra and Its Applications 438, 4296 - 4321.
- [8] Sturmfels, B., 1994. On The Newton Polytope of the Resultant. Journal of Algebraic Combinatorics, 3, 207-236.

---

---

# Session 4: Computer Algebra in Coding Theory and Cryptography

---

---

Organizers:

Ilias Kotsireas  
Edgar Martínez-Moro



# A characterization of cyclic codes whose minimum distance equals their maximum BCH bound\*

José Joaquín Bernal and Juan Jacobo Simón  
University of Murcia (Spain)

Diana H. Bueno-Carreño  
Pontificia Universidad Javeriana-Cali (Colombia)

(josejoaquin.bernal,jsimon,dianahaidive.bueno)@um.es

## Abstract

In this extended abstract we characterize those cyclic codes for which its minimum distance reaches the maximum of its BCH bounds. We also study a constructive point of view by means of computations of divisors of a polynomial of the form  $x^n - 1$ . We apply our results to the study of those BCH codes  $C$ , with designed distance  $\delta$  that have true minimum distance  $d(C) = \delta$ . Finally, we present some examples of new binary BCH codes with true minimum distance. To do this, we make use of two related tools: the discrete Fourier transform and the notion of apparent distance of a code, originally defined for multivariate abelian codes.

## Keywords

Cyclic codes, BCH bound, apparent distance, true minimum distance

## 1 Introduction

To compute the minimum distance of cyclic codes, or a lower bound for them, is one of the most studied problems in abelian codes (see, for example, [3, 5, 6]). The oldest lower bound for the minimum distance of a cyclic code is the BCH bound [4, p. 151]. The study of this bound and its generalizations is a classical topic, which includes the study of the very well-known family of BCH codes. Within them, an interesting problem is to determine, for a given code, when the maximum of its BCH bounds equals its minimum distance (see [2, 5]). This is our interest.

In this extended abstract we state conditions on a cyclic code for its minimum distance equals the maximum of its BCH bounds. To do this, we make use of two related tools; to wit, the discrete Fourier transform and the notion of apparent distance of a code, originally defined for multivariate abelian codes in [1]. These tools and all notation are given in Section 2. In Section 3, we characterize those cyclic codes for which its minimum distance reaches the maximum of its BCH bounds. Then we study a constructive point of view by means of computations of divisors of a polynomial of the form  $x^n - 1$ . In Section 4, we apply our results to the study of those BCH codes  $C$ , with designed distance  $\delta$ , that have true minimum distance  $d(C) = \delta$  (see [5, Section 9.2]). Finally, some examples of new binary BCH codes with true minimum distance are presented.

## 2 Notation and preliminaries

We will use standard terminology from coding theory (see, for example [5, Chapter 7] or [2, Section 2]). We denote by  $q$  a power of a prime number  $p$  and by  $\mathbb{F} = \mathbb{F}_q$  the field of  $q$ -elements. Let  $n$  be a positive integer which is coprime to  $q$  and let  $\mathbb{L}/\mathbb{F}$  an extension field containing a  $n$ -th primitive root of unity, say  $\alpha$ , that we fix throughout this note.

---

\*This work was partially supported by MINECO (Ministerio de Economía y Competitividad), (Fondo Europeo de Desarrollo Regional) project MTM2012-35240 and Fundación Séneca of Murcia. The second author has been supported by Departamento Administrativo de Ciencia, Tecnología e Innovación de la República de Colombia

We denote by  $\mathbb{F}[x]$  the ring of polynomials with coefficients in  $\mathbb{F}$ . For any polynomial  $g = g(x) \in \mathbb{F}[x]$  we denote by  $\deg(g)$  its degree and by  $\text{supp}(g)$  its support. Instead of working with group rings, we consider the polynomial  $x^n - 1 \in \mathbb{F}[x]$  and form the quotient ring  $\mathbb{F}[x]/(x^n - 1)$ , which we denote by  $\mathbb{F}(n)$ . As usual, we identify the elements  $g \in \mathbb{F}(n)$  with polynomials; so that we may take  $g \in \mathbb{F}(n)$  and then write  $g \in \mathbb{F}[x]$  (where  $\deg(g) < n$ ). In case we first consider a polynomial  $f \in \mathbb{F}[x]$ , possibly with  $\deg(f) \geq n$ , then we denote by  $\bar{f}$  its image under the canonical projection onto  $\mathbb{F}(n)$ .

A cyclic code  $C$  of length  $n$  in the alphabet  $\mathbb{F}$  will be identified with its corresponding ideal in  $\mathbb{F}(n)$  (up to permutation equivalence). It is well known that, when  $\gcd(n, q) = 1$ , the quotient ring  $\mathbb{F}(n)$  is semisimple and then every cyclic code has a unique monic generator polynomial [5, Theorem 7.1] and a unique generator idempotent [5, Theorem 8.1]. We always assume that  $\gcd(n, q) = 1$ .

It is well known that every cyclic code  $C$  of  $\mathbb{F}(n)$  is totally determined by its root set (or the zeros of the code), which is defined as  $Z(C) = \{\alpha^i \mid c(\alpha^i) = 0 \text{ for all } c \in C\}$ ; that is, for any polynomial  $f \in \mathbb{F}(n)$ , we have that  $f \in C$  if and only if  $f(\beta) = 0$  for all  $\beta \in Z(C)$ . We denote the defining set of  $C$  as  $D(C) = \{i \in \mathbb{Z}_n \mid \alpha^i \in Z(C)\}$  [5, p. 199]. It is well-known that defining sets are partitioned in  $q$ -cyclotomic cosets modulo  $n$  [5, p.104]; that is, denoting by  $\mathbb{Z}_n$ , the integers modulo  $n$ , and given any element  $a \in \mathbb{Z}_n$ , the  $q$ -cyclotomic coset of  $a$ , modulo  $n$  is the set  $C_q(a) = \{a, qa, \dots, q^{n_a-1}a\}$ , where  $n_a$  is the smallest positive integer such that  $q^{n_a}a \equiv a \pmod n$ . We recall that the notions of set of zeros and defining set are also applied to polynomials in  $\mathbb{F}(n)$ .

For any code  $C$ , we denote its minimum distance by  $d(C)$ . The BCH bound states that for any cyclic code that has a string of  $\delta - 1$  consecutive powers of  $\alpha$  as zeros, the minimum distance of the code is at least  $\delta$  [5, Theorem 7.8]. Clearly, for any cyclic code  $C$  there exists the maximum of its BCH bounds, that we denote by  $\Delta(C)$ . Some times it is called *the* BCH (lower) bound of the code (see [1, p. 22] and [2, p. 984]).

A cyclic code  $C$  of  $\mathbb{F}(n)$ , with polynomial generator  $g(x)$ , is a BCH code of designed distance  $\delta$  if  $g(x)$  is the polynomial with the lowest degree over  $\mathbb{F}$  having  $\{\alpha^{b+j} \mid j = 0, \dots, \delta - 2\} \subseteq Z(C)$  (see [5, p. 202]) or, equivalently if for any cyclotomic coset  $Q \subseteq D(C)$  we have that  $Q \cap \{b + j \mid j = 0, \dots, \delta - 2\} \neq \emptyset$ . The Bose distance is defined for a BCH code  $C$  of designed distance  $\delta$ , as the largest  $\delta'$  such that  $C$  is a BCH code of designed distance  $\delta'$ . Note that for a BCH code  $C$  it may happens that its Bose distance being less than  $\Delta(C)$ , as the following example shows.

**Example 1.** Set  $q = 2$ ,  $n = 31$  and  $\alpha$  a 31-th primitive root of unity. Let  $C$  be the BCH code generated by  $\text{lcm}\{M^{(15)}, M^{(16)}, M^{(17)}\}$ , where  $M^{(t)}$ , denotes the minimal polynomial of  $\alpha^t$  in  $\mathbb{F}[x]$ . Consider the 2-cyclotomic cosets  $C_1 = \{1, 2, 4, 8, 16\}$ ,  $C_3 = \{3, 6, 12, 17, 24\}$  and  $C_{15} = \{15, 23, 27, 29, 30\}$ . Then one may check that the defining set of the code  $C$  is  $D(C) = C_1 \cup C_3 \cup C_{15}$ , and that the Bose distance is  $\delta = 4$ . However  $\Delta(C) = 5$ , because  $\{1, 2, 3, 4\} \subset D(C)$ . But  $\{1, 2, 3, 4\} \subset C_1 \cup C_3$ , so that  $C$  cannot be a BCH code of designed distance  $\delta = 5$ . Hence the Bose distance is less than the maximum of all possible BCH bounds (or simply, the BCH bound,  $\Delta(C)$ ).

Let  $\mathbb{L}/\mathbb{F}$  an extension field that contains a  $n$ -th primitive root of unity,  $\alpha$ . The (discrete) Fourier transform of a polynomial  $f \in \mathbb{F}(n)$  (also called Mattson-Solomon polynomial), that we denote by  $\varphi_f$  is defined as  $\varphi_f(x) = \sum_{j=0}^{n-1} f(\alpha^j) X^j$ . Clearly,  $\varphi_f \in \mathbb{L}(n)$ ; moreover, the Fourier transform may be viewed as an isomorphism of algebras  $\varphi : \mathbb{L}(n) \rightarrow (\mathbb{L}^n, \star)$ , where the multiplication “ $\star$ ” in  $\mathbb{L}^n$  is defined coordinatewise (see [1, Section 2.2] or [5, § 8.6]). The inverse of the Fourier transform is given by  $\varphi_g^{-1} = \frac{1}{n} \sum_{i=0}^{n-1} g(\alpha^{-i}) X^i$  (see for details any of [1, 2, 5]).

Let us recall some definitions in [1, Chapter 3] related to the computation of the BCH bound. The context of these definitions is the study of multivariate polynomials, so, for the sake of simplicity, we present a very simplified version only concerning univariate polynomials.

**Definition 2.** Let  $\mathbb{L}/\mathbb{F}$  an extension field that contains a  $n$ -th primitive root of unity,  $\alpha$ . For any element  $g \in \mathbb{L}(n)$  we define the apparent distance of  $g$ , that we denote  $d^*(g)$ , as follows.

1. If  $g = 0$  then  $d^*(0) = 0$ .
2. If  $g \neq 0$  then

$$d^*(g) = \max \left\{ n - \deg \left( \overline{x^h g} \right) \mid 0 \leq h \leq n - 1 \right\}.$$

Now, the apparent distance of a cyclic code  $C$  in  $\mathbb{F}(n)$  with generator idempotent  $e \in C$  is  $d^*(C) = d^*(\varphi_e)$  and moreover

$$\Delta(C) = d^*(C) = d^*(\varphi_e) \leq d(C) \quad (1)$$

(see [1, p. 22]). As an immediate consequence we have.

**Corollary 3.** *Notation as above. Let  $C$  be a cyclic code in  $\mathbb{F}(n)$  with generator idempotent  $e \in C$ . If  $d^*(\varphi_e) = \omega(e)$  then  $d(C) = \Delta(C)$ .*

### 3 The minimum distance and the BCH bound

We keep all notation of the preceding section. For an arbitrary element  $g \in \mathbb{L}(n)$ , which we may view as a polynomial with  $\deg(g) \leq n - 1$  and for any  $h \in \{0, \dots, n - 1\}$  we write

$$m_g = \gcd(x^h g, x^n - 1) \quad (2)$$

where  $m_g$  does not depend on  $h$ , because  $x^h$  and  $x^n - 1$  are relatively prime polynomials. We also write, for any  $h \in \{0, \dots, n - 1\}$

$$x^h g = (x^n - 1)f_{g,h} + \overline{x^h g} \quad (3)$$

where  $f_{g,h}$  is a suitable quotient from the division algorithm. Note that if  $g \neq 0$  then  $\overline{x^h g} \neq 0$  because  $\deg(g) < n$ . By using results in [1] and [3] (see also [5, Theorem 8.6.31]) we may get the following result.

**Lemma 4.** *Let  $n, q, \mathbb{F}$  and  $\mathbb{L}$  be as above. Consider  $g \in \mathbb{L}(n)$  and let  $m_g$  be as above. Then*

1.  $d^*(g) \leq n - \deg(m_g)$ .
2. If  $g \mid x^n - 1$  then  $d^*(g) = n - \deg(g)$ .

As a direct consequence we have the following result (see [1, Theorem 4.1] and [3, Theorem 2]).

**Corollary 5.** *Let  $C$  be a cyclic code in  $\mathbb{F}(n)$  and  $c \in C$ . Then*

1.  $d^*(\varphi_c) \leq \omega(c)$ .
2.  $n - \deg(m_{\varphi_c}) = \omega(c)$ .

Then, by lemma above, the apparent distance of any  $f \in \mathbb{L}(n)$  is less than or equal to the number of nonzeros of  $m_f$ . The following result shows us when the equality is reached.

**Proposition 6.** *Let  $n, q, \mathbb{F}$  and  $\mathbb{L}$  be as above. Consider  $f \in \mathbb{L}(n)$  and let  $m_f$  be as in (2). Then  $d^*(f) = n - \deg(m_f)$  if and only if there exists  $h \in \{0, \dots, n - 1\}$  such that  $\overline{x^h f} \mid x^n - 1$  (equivalently,  $\overline{x^h f}$  and  $m_f$  are associated polynomials in  $\mathbb{L}[x]$ ).*

Now, our main result.

**Theorem 7.** *Let  $n$  be a positive integer,  $p$  a prime number and  $q$  a power of  $p$ . Assume that  $\gcd(n, q) = 1$ . Consider the field  $\mathbb{F}$  and an extension field  $\mathbb{L}/\mathbb{F}$  containing a  $n$ -th primitive root of unity  $\alpha$ . Let  $C$  be a cyclic code in  $\mathbb{F}(n)$ . Then  $d(C) = \Delta(C)$  if and only if there exists a polynomial  $f \in \mathbb{L}(n)$ , such that*

1.  $d^*(f) = d^*(C)$ .
2.  $d^*(f) = n - \deg(m_f)$
3.  $\varphi_f^{-1} \in C$ .

Moreover, in this case, there exists  $h \in \{0, \dots, n - 1\}$  such that  $\overline{x^h f} \mid x^n - 1$ .

Under a constructive point of view, the theorem above together with Proposition 6 shows us that we only have to focus on the divisors of  $x^n - 1$ . Let us state this fact in the following results that we will use in the next section.

**Corollary 8.** *Hypotheses as in Theorem 7. Let  $C$  be a cyclic code in  $\mathbb{F}(n)$ . Then  $d(C) = \Delta(C)$  if and only if there exists  $k \in \{0, \dots, n - 1\}$  and a divisor  $g \mid x^n - 1$ , in  $\mathbb{L}[x]$ , such that setting  $f = \overline{x^k g}$ , the following conditions hold.*

1.  $d^*(f) = d^*(C)$  (recall that  $d^*(f) = d^*(g)$ ).
2.  $\varphi_f^{-1} \in C$ .

**Example 9.** Set  $q = 2$ ,  $n = 45$  and  $g = x^{40} + x^{39} + x^{38} + x^{36} + x^{35} + x^{32} + x^{30} + x^{25} + x^{24} + x^{23} + x^{21} + x^{20} + x^{17} + x^{15} + x^{10} + x^9 + x^8 + x^6 + x^5 + x^2 + 1$ . Let  $\alpha$  be a 45-th primitive root of unity. To find the parameter  $k$  in the corollary above, we have to compute  $g(1)$  and  $g(\alpha^3)$ , because the defining set of the polynomial  $(x^{45} - 1)/g$  is  $C_2(0) \cup C_2(3)$ . Since  $g(1) = 1$  and  $g(\alpha^3) = \alpha^{30}$  then  $k = 15$  works. That is, setting  $f = x^{15}g$  we have that  $\varphi_f^{-1} \in \mathbb{F}(45)$ . Set  $C = (\varphi_f^{-1})$  and we have that  $5 = d(C) = \Delta(C)$  and  $\dim(C) = 21$ . In fact,  $C$  is a BCH code with  $\delta = 5$ .

It is well-known that, under our notation,  $a \in \mathbb{L}$  verifies that  $a \in \mathbb{F}$  if and only if  $a^q = a$ .

**Corollary 10.** *Hypotheses as in Theorem 7. Let  $C$  be a cyclic code in  $\mathbb{F}(n)$ . Then  $d(C) = \Delta(C)$  if and only if there exists  $k \in \{0, \dots, n-1\}$  and a divisor  $g \mid x^n - 1$ , in  $\mathbb{L}[x]$ , such that the following conditions hold.*

1.  $d^*(g) = d^*(C)$ , and setting  $f = \overline{x^k g}$ ,
2.  $\text{supp}(f) \subseteq \mathbb{Z}_n \setminus D(C)$ ,
3.  $(f(\alpha^j))^q = f(\alpha^j)$ , for any  $j \in \{0, \dots, n-1\}$ ,

Now we give a sufficient condition to get BCH codes yielding its true minimum distance.

**Corollary 11.** *Let  $C$  be a cyclic code in  $\mathbb{F}(n)$  with generator idempotent  $e \in C$ . If there exists  $h \in \{0, \dots, n-1\}$  such that  $\overline{x^h \varphi_e} \mid x^n - 1$  then  $d(C) = \Delta(C)$ .*

## 4 Applications: true minimum distance in BCH codes

We keep all notation. The following result allows us to construct BCH codes  $B(\delta)$ , for which  $d(B(\delta)) = \Delta(B(\delta)) = \delta$ . We recall that, for a given polynomial  $g \in \mathbb{F}(n)$ , it is denoted by  $(g)$  the ideal in  $\mathbb{F}(n)$  generated by  $g$ .

**Proposition 12.** *Let  $g \in \mathbb{L}[x]$  be a divisor of  $x^n - 1$ . If  $\varphi_{x^k g}^{-1}$  belongs to  $\mathbb{F}[x]$ , for some  $k \in \{0, \dots, n-1\}$ , then the cyclic code  $C = \left(\varphi_{x^k g}^{-1}\right)$  verifies that  $\Delta(C) = d(C)$ .*

**Theorem 13.** *Let  $g \in \mathbb{L}[x]$  be a divisor of  $x^n - 1$ . If there exists  $k \in \{0, \dots, n-1\}$ , such that  $\overline{x^k g(\alpha^j)} \in \mathbb{F}$ , for all  $j = 0, \dots, n-1$  then there exists a BCH code of designed distance  $\delta$ ,  $C = B(\delta)$  (containing  $\varphi_{x^k g}^{-1}$ ) such that  $\delta = \Delta(C) = d(C) = n - \deg(g)$ .*

For any couple of positive integers  $a, b$ , we denote by  $O_a(b)$  the multiplicative order of  $b$ , modulo  $a$ . We also denote by  $\phi(a)$  the Euler's totient function.

**Theorem 14.** *Let  $n$  be a positive integer,  $p$  a prime number and  $q$  a power of  $p$ . Assume that  $\gcd(n, q) = 1$ . Consider the field  $\mathbb{F}$  and an extension field  $\mathbb{L}/\mathbb{F}$  containing a  $n$ -th primitive root of unity  $\alpha$ . Let  $h$  be an irreducible factor of  $x^n - 1$  with defining set  $D(h)$ . We set  $g = (x^n - 1)/h$  and pick any  $j \in D(h)$ . If  $g(\alpha^j) = \alpha^k$  then there exists a BCH code of designed distance  $\delta$ ,  $C = B(\delta)$  such that  $\delta = \Delta(C) = d(C) = \deg(h)$ .*

**Corollary 15.** *Let  $n = q^m - 1$ , for some  $m \in \mathbb{N}$ . For each divisor  $l$  of  $n$ , there exist  $\frac{\phi(l)}{O_l(q)}$  BCH codes of designed distance  $\delta = O_l(q)$  over  $\mathbb{F}$  having true minimum distance  $\delta$ .*

**Example 16.** Set  $q = 2$  and  $n = 15$ . Denote the irreducible factors by  $h_1 = \Phi_1$ ,  $h_2 = \Phi_3$ ,  $h_3 = x^4 + x + 1$ ,  $h_4 = x^4 + x^3 + 1$  and  $h_5 = \Phi_5$ .

Setting  $g_i = \frac{x^n - 1}{h_i}$  we apply Theorem 14 above to get the following table of BCH codes of length 15 having true minimum distance  $\delta$ .

Factor	Dimension	$\delta = d$
$g_1$	15	1
$g_2$	10	2
$g_3$	8	4
$g_4$	8	4
$g_5$	6	4



Note that the codes associated to  $g_2, \dots, g_5$  are not considered in the classical result [5, Theorem 9.2.5]. There are more nonconsidered codes. The polynomial  $g = \Phi_{15}\Phi_5$  verifies the conditions of Theorem 13 with  $k = 0$ , and hence it determines a BCH code,  $C_6$  having true minimum distance  $\delta$ , with parameters  $\dim(C) = 5$  and  $d(C) = 3$ . Also  $\Phi_5\Phi_3h_3$  verifies the conditions of Theorem 13 with  $k = 0$ , and hence it determines a BCH code  $C_7$  having true minimum distance  $\delta$ , with parameters  $\dim(C) = 7$  and  $d(C) = 5$ .

**Example 17.** Set  $q = 2$  and  $n = 21$ . Denote the irreducible factors by  $h_1 = \Phi_1$ ,  $h_2 = \Phi_3$ ,  $h_3 = x^3 + x + 1$ ,  $h_4 = x^3 + x^2 + 1$ ,  $h_5 = x^6 + x^4 + x^2 + x + 1$  and  $h_6 = x^6 + x^5 + x^4 + x^2 + 1$

Setting  $g_i = \frac{x^n - 1}{h_i}$  we apply Theorem 14 above to get the following table of binary BCH codes of length 21 having true minimum distance  $\delta$ . We complete with another one satisfying the conditions of Theorem 13.

Factor	Dimension	$\delta = d$
$g_1$	21	1
$g_2$	14	2
$g_3$	12	3
$g_4$	12	3
$g_5$	8	6
$g_6$	8	6
$\Phi_{21}h_3h_1$	10	6

We finish with an example of a binary BCH code with true minimum distance  $\delta$  of length 33. We have not found in the literature any binary BCH code having this length.

**Example 18.** Set  $q = 2$ ,  $n = 33$  and  $g = x^{30} + x^{27} + x^{24} + x^{21} + x^{18} + x^{15} + x^{12} + x^9 + x^6 + x^3 + 1$ . One may check that  $g$  verifies the conditions of Theorem 13 with  $k = 0$ , and hence it determines a BCH code  $C$  having true minimum distance  $\delta$ , with parameters  $\dim(C) = 11$  and  $d(C) = 3$ .

## References

- [1] P. Camion, Abelian Codes, MRC Tech. Sum. Rep. 1059, Univ. of Wisconsin, Madison, 1970.
- [2] Charpin, P., Open Problems on Cyclic Codes. in V. S. Pless, W. C. Huffman and R. A. Brualdi (editors) *Handbook of Coding Theory* vol. I. North-Holland, Amsterdam, 1998.
- [3] R. T. Chien and D. M. Chow, Algebraic Generalization of BCH-Goppa-Helgert Codes, IEEE Trans. Inform. Theory, vol. 21, no. 1, 1975.
- [4] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge, 2003.
- [5] F.J. Macwilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Mathematical Library, 1977.
- [6] J. H. Van Lint and R. M. Wilson, On the Minimum Distance of Cyclic Codes, IEEE Trans. Inform. Theory, vol. 32, no. 1, 1986.

# Gröbner Bases and Linear Codes over Prime Fields

Natalia Dück, Karl-Heinz Zimmermann  
Hamburg University of Technology (Germany)

natalia.dueck@tuhh.de

## Abstract

In this short paper, a link between Gröbner bases and linear codes over prime fields will be established by associating to each linear code the so-called code ideal which is a binomial ideal given as the sum of toric ideal and a non-prime ideal.

An algorithm using Gröbner basis techniques will be presented that computes a basis for a subspace of a finite-dimensional vector space over a finite prime field given as a matrix kernel which is an adaptation of the Gröbner basis based method used to calculate the Hilbert basis of a numerical submonoid. Furthermore, results concerning the universal Gröbner basis of the code ideals will be given. In particular, it will be shown that for binary codes the universal Gröbner basis consists of all binomials associated to codewords whose Hamming weight satisfies the Singleton bound and a particular rank condition. This will give rise to a new class of binary linear codes called Singleton codes.

## Keywords

Linear code, Gröbner basis, universal Gröbner basis, binomial ideal, toric ideal

## 1 Introduction

Digital data are exposed to errors when transmitted through a noisy channel. But as receiving correct data is indispensable in many applications, error-correcting codes are employed to tackle this problem. By adding redundancy to the messages, errors can be detected and corrected. Since the late 1940's the study of such codes is an ongoing and important task.

Gröbner bases, on the other hand, are a powerful tool that has originated from commutative algebra providing a uniform approach to grasp a wide range of problems such as solving algebraic systems of equations, ideal membership, and effective computation in residue class rings modulo polynomial ideals [1, 2]. Additionally, Gröbner basis techniques also provide means of solving problems in integer programming and invariant theory.

Both disciplines can be linked by associating a linear code over a prime field with a binomial ideal given as the sum of a toric ideal and a non-prime ideal called code ideal. In this way, several concepts from the rich theory of toric ideals can be translated into the setting of code ideals. This idea stems from [4] and has already proven its value in the binary case as it allows for determining the error-correcting capabilities of a binary linear code.

In this short paper, some connections between Gröbner bases and linear codes over prime fields will be established. As a first application we will give an algorithm using Gröbner basis techniques which computes a basis for a subspace of a finite-dimensional vector space over a finite prime field given as a matrix kernel [5]. In fact, this algorithm is an adaptation of the Gröbner basis based method used to calculate the Hilbert basis of a numerical submonoid [10]. This is of particular interest in the context of linear codes over prime fields. Using this method a generator matrix for such a code can be computed that is described by its parity check matrix.

The second part is devoted to the universal Gröbner basis of the code ideal. Gröbner bases are an essential tool for utilizing ideals in computer algebra systems. But as Gröbner bases vary with the monomial order and distinct applications require different monomial orders, it is advantageous to know the universal Gröbner basis, i.e., a finite generating set of the ideal which is a Gröbner basis for all monomial orders. For toric ideals this problem has been solved and an algorithm for computing the universal Gröbner basis has been provided [9]. For the code ideal, however, this problem remains unsolved. To this end several concepts used in connection with toric ideals will be adapted. In particular, it will be shown that for binary linear codes the universal Gröbner basis can be completely described by a linear algebraic rank condition.

## 2 Computing the Kernel of a Matrix over a Finite Field

Let  $\mathcal{A}$  be an  $m \times n$  matrix with entries in  $\mathbb{Z}$  and denote by  $\Lambda(\mathcal{A})$  its Lawrence lifting. For any  $u \in \mathbb{Z}$  write  $u^+ = \max\{u, 0\}$  and  $u^- = \max\{-u, 0\}$  and for any vector  $v \in \mathbb{Z}^n$  define  $v^+$  and  $v^-$  componentwise. Clearly,  $v = v^+ - v^-$ , where  $v^+, v^- \in \mathbb{N}_0^n$  have disjoint support.

It is well-known that the toric ideal  $I(\mathcal{A})$  associated to the matrix  $\mathcal{A}$  is generated by pure binomials  $\mathbf{x}^{v^+} - \mathbf{x}^{v^-}$ , where  $v^+ - v^-$  belongs to  $\ker_{\mathbb{Z}}(\mathcal{A})$ , and that there is a bijection between pure binomials in  $I(\mathcal{A})$  and  $I(\Lambda(\mathcal{A}))$  by mapping  $\mathbf{x}^u - \mathbf{x}^v$  to  $\mathbf{x}^u \mathbf{y}^v - \mathbf{x}^v \mathbf{y}^u$ . It follows that if  $u \in \ker_{\mathbb{Z}}(\mathcal{A}) \cap \mathbb{N}_0$ , then the binomial  $\mathbf{x}^u - \mathbf{y}^u$  belongs to  $I(\Lambda(\mathcal{A}))$  [3, 8, 9]. This gives the foundation for an algorithm computing the Hilbert basis of the submonoid  $\ker_{\mathbb{Z}}(\mathcal{A}) \cap \mathbb{N}_0$  using Gröbner bases [10].

In the following, let  $\mathbb{F}_p$  denote a finite field with  $p$  elements, where  $p$  is a prime. We will provide an adaptation of the above mentioned Hilbert basis algorithm for finding a basis of the subspace

$$\ker(H) := \ker(H_p) \subset \mathbb{F}_p^n, \quad (1)$$

where  $H$  is an  $m \times n$  integer matrix and  $H_p = H \otimes_{\mathbb{Z}} \mathbb{F}_p$ .

In order to account for  $p = 0$  in  $\mathbb{F}_p$ , the following ideal will be used

$$I_p(\mathbf{x}) = \langle x_i^p - 1 \mid 1 \leq i \leq n \rangle.$$

In this way, the exponents of the monomials can be treated as vectors in  $\mathbb{F}_p^n$ .

Let  $H = (h_{ij})$  be an  $m \times n$ -matrix with entries in  $\mathbb{F}_p$  and define the ideals

$$J_H = \left\langle v_j - w_j \prod_{i=1}^m x_i^{h_{ij}} \mid 1 \leq j \leq n \right\rangle \quad (2)$$

and

$$I_H = J_H + I_p(\mathbf{x}) + I_p(\mathbf{v}) + I_p(\mathbf{w}). \quad (3)$$

Furthermore, define the mapping  $\psi : \mathbb{K}[v_1, \dots, v_n, w_1, \dots, w_n] \rightarrow \mathbb{K}[x_1, \dots, x_m, w_1, \dots, w_n]$  on the variables first

$$\psi(v_j) = w_j \prod_{i=1}^m x_i^{h_{ij}} \quad \text{and} \quad \psi(w_j) = w_j, \quad 1 \leq j \leq n, \quad (4)$$

and then extend it such that it becomes a ring homomorphism. Obviously,  $\ker(\psi) = J_H \cap \mathbb{K}[\mathbf{v}, \mathbf{w}]$ . This homomorphism can be used to detect elements in the kernel of  $H$ .

**Lemma 2.1.** *If  $\alpha, \alpha', \beta, \beta' \in \mathbb{F}_p^n$  with  $\alpha' - \alpha = \beta - \beta'$  in  $\mathbb{F}_p^n$ , then  $\alpha' - \alpha \in \ker(H)$  if and only if*

$$\psi(\mathbf{v}^{\alpha'} \mathbf{w}^{\beta'} - \mathbf{v}^{\alpha} \mathbf{w}^{\beta}) = 0 \quad \text{mod} \quad (I_p(\mathbf{x}) + I_p(\mathbf{v}) + I_p(\mathbf{w})). \quad (5)$$

Indeed, this result also holds when the field  $\mathbb{F}_p$  is replaced by  $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ , where  $m$  is an arbitrary positive integer [6].

Note that each nonzero vector  $\alpha \in \mathbb{F}_p^n$  can be written as  $\alpha = (0, \dots, 0, \alpha_i, \bar{\alpha})$ , where  $\alpha_i \in \mathbb{F}_p \setminus \{0\}$  and  $\bar{\alpha} \in \mathbb{F}_p^{n-i}$ . Put  $\alpha' = \alpha_i \mathbf{e}_i - \alpha = (0, \dots, 0, 0, -\bar{\alpha})$ , where  $\mathbf{e}_i$  is the  $i$ th unit vector.

**Theorem 2.2.** *Let  $\mathcal{G}$  be a Gröbner basis for  $I_H$  w.r.t. the lexicographical order with  $x_1 \succ \dots \succ x_m \succ v_1 \succ \dots \succ v_n \succ w_1 \succ \dots \succ w_n$ . Then a basis for  $\ker(H)$  in  $\mathbb{F}_p^n$  is given by*

$$\mathcal{H} = \left\{ (0, \dots, 0, \alpha_i, \bar{\alpha}) \in \mathbb{F}_p^n \mid v_i^{\alpha_i} - \mathbf{v}^{\alpha'} \mathbf{w}^{\bar{\alpha}} \in \mathcal{G}, \alpha' = \alpha_i \mathbf{e}_i - \alpha, \alpha_i \neq 0, 1 \leq i \leq n \right\}. \quad (6)$$

This result provides an algorithm for computing a basis of the matrix kernel over a finite prime field. Moreover, if this algorithm is applied to  $\mathbb{Z}_m$  where  $m$  is not prime, it yields a module basis when  $\ker(H)$  is a free  $\mathbb{Z}_m$ -module and a generating set in row reduced echelon form when it is not free.

There are several differences between this adaptation and the original method. First, Hilbert bases for submonoids are unique as opposed to bases for vector spaces. Thus in the first case, the unique Hilbert basis is computed. In the second case, however, a specific vector space basis is calculated, namely the one which is in reduced row echelon form with respect to the first  $m$

columns. Indeed, changing the lexicographic order  $x_1 \succ \dots \succ x_m$  to  $x_{i_1} \succ \dots \succ x_{i_m}$  yields a basis in reduced row echelon form with respect to the columns  $i_1, i_2, \dots, i_m$ .

Second, in the algorithm for computing the Hilbert basis the set  $\mathcal{H}$  is constructed by selecting binomials of the form  $\mathbf{v}^\alpha - \mathbf{w}^\alpha$  from the Gröbner basis which is justified by the fact that every pure binomial in the ideal  $I(\Lambda(\mathcal{A}))$  has the shape  $\mathbf{v}^\alpha \mathbf{w}^\beta - \mathbf{v}^\beta \mathbf{w}^\alpha$ . However, adding the ideals  $I_p(\mathbf{x}), I_p(\mathbf{v})$  and  $I_p(\mathbf{w})$  produces an ideal which also contains pure binomials  $\mathbf{v}^\alpha \mathbf{w}^\beta - \mathbf{v}^{\alpha'} \mathbf{w}^{\beta'}$  with  $\alpha - \alpha' = \beta' - \beta$  but possibly  $\alpha \neq \beta'$  and  $\alpha' \neq \beta$  in  $\mathbb{F}_p^n$ .

Finally, the proposed method is rather unefficient when compared to other known methods from linear algebra since computation of Gröbner bases can be rather costly. Nevertheless it is of interest from the theoretical point of view because it demonstrates the extension to the finite module case.

### 3 Universal Gröbner Basis for the Code Ideal

For an  $[n, k]$  code  $\mathcal{C}$  over a prime field  $\mathbb{F}_p$  define the associated *code ideal* to be

$$I_{\mathcal{C}} = \langle \mathbf{x}^c - \mathbf{x}^{c'} \mid c - c' \in \mathcal{C} \rangle + I_p(\mathbf{x}) \subset \mathbb{K}[x_1, \dots, x_n], \quad (7)$$

where  $\mathbb{K}$  is an arbitrary field. As in the previous section  $I_p(\mathbf{x})$  allows to view the exponents of the monomials as vectors in  $\mathbb{F}_p^n$ . This ideal can be based on a toric ideal as follows,

$$I_{\mathcal{C}} = I_A + I_p(\mathbf{x}), \quad (8)$$

where  $A$  in an integral  $n - k \times n$  matrix such that  $H = A \otimes_{\mathbb{Z}} \mathbb{F}_p$  is a parity check matrix for  $\mathcal{C}$ . This shows that  $I_{\mathcal{C}}$  is given as the sum of a toric ideal and a non-prime ideal.

Clearly, the ideal  $I_{\mathcal{C}}$  is generated by pure binomials  $\mathbf{x}^c - \mathbf{x}^{c'}$  with  $c - c' \in \mathcal{C}$ . Thus, in what follows binomials will always be considered to be pure. A binomial  $\mathbf{x}^c - \mathbf{x}^{c'}$  in  $I_{\mathcal{C}}$  is said to be associated to the codeword  $c - c'$ , but unlike for a toric ideal, there is more than one binomial associated to a codeword since the decomposition  $c = c^+ - c^-$  is not unique. This is one of the main reasons why results concerning toric ideals cannot be translated one-to-one to this setting.

In [9] the author has introduced several concepts in the context of toric ideals which will be utilized in the following. Because of the mentioned subtleties, however, several of these concepts need to be adapted.

A binomial  $\mathbf{x}^c - \mathbf{x}^{c'}$  in  $I_{\mathcal{C}}$  is called *primitive* if there is no other binomial  $\mathbf{x}^u - \mathbf{x}^{u'}$  in  $I_{\mathcal{C}}$  such that  $\mathbf{x}^u$  divides  $\mathbf{x}^c$  and  $\mathbf{x}^{u'}$  divides  $\mathbf{x}^{c'}$ . If  $\mathcal{C}$  is a binary code then we additionally require  $c' \neq \mathbf{0}$ . The *Graver basis* for  $\mathcal{C}$  consists of all primitive binomials lying in the corresponding code ideal and is denoted by  $\text{Gr}_{\mathcal{C}}$ .

A binomial  $\mathbf{x}^c - \mathbf{x}^{c'}$  in  $I_{\mathcal{C}}$  is called a *circuit* if it is a primitive binomial and its support is minimal with respect to inclusion. Denote by  $C_{\mathcal{C}}$  the set of all circuits of the ideal  $I_{\mathcal{C}}$ . Finally, denote the universal Gröbner basis by  $\mathcal{U}_{\mathcal{C}}$ .

The binary and non-binary case differ substantially. In the binary case, being a circuit is a property which only depends on the codeword associated to the binomial. To be more precise, the binomial  $\mathbf{x}^c - \mathbf{x}^{c'}$  is a circuit if and only if the associated codeword  $c - c'$  has minimal support w.r.t. inclusion. In other words, if one expansion  $c = c^+ - c^-$  yields a circuit, then every expansion of  $c$  is a circuit and the same is true for being primitive. In the non-binary situation, however, this is not true as is illustrated next.

**Example 1.** Consider the linear code  $\mathcal{C}$  over  $\mathbb{F}_7$  generated by  $G = \begin{pmatrix} 1 & 0 & 4 \\ 0 & 1 & 1 \end{pmatrix}$  and the corresponding code ideal  $I_{\mathcal{C}}$  in  $\mathbb{Q}[a, b, c]$ . The codeword  $(2, 6, 0)$  has minimal support. Expanding  $(2, 6, 0) = (2, 0, 0) - (0, 1, 0)$  gives the circuit  $a^2 - b$ . However, writing  $(2, 6, 0) = (0, 6, 0) - (5, 0, 0)$  yields the binomial  $b^6 - a^5$  which is not even primitive because  $b^2 - a^4$  also belongs to  $I_{\mathcal{C}}$ .

**Proposition 3.1.** For a linear code  $\mathcal{C}$  over  $\mathbb{F}_p$ ,  $C_{\mathcal{C}} \subseteq \mathcal{U}_{\mathcal{C}} \subseteq \text{Gr}_{\mathcal{C}}$ .

Note that the same inclusions are obtained for toric ideals [9]. For non-binary linear codes, these inclusions can be strict. For binary linear codes, however, all three sets coincide.

**Theorem 3.2.** For a binary linear code  $\mathcal{C}$  the set of circuits  $C_{\mathcal{C}}$  equals the Graver basis  $\text{Gr}_{\mathcal{C}}$ .

For a binary  $[n, k]$  code  $\mathcal{C}$  one can even further describe all primitive binomials in the code ideal  $I_{\mathcal{C}}$ . If  $\mathbf{x}^c - \mathbf{x}^{c'}$  is primitive, then  $\text{wt}(c - c') \leq n - k + 1$  and for any generator matrix  $G$  of the code  $\mathcal{C}$  the submatrix  $G_{\underline{n} \setminus \text{supp}(c - c')}$  has rank  $k - 1$ . And the converse is also true, i.e., if  $c$  is a codeword of Hamming weight less than or equal to  $n - k + 1$  and such that  $G_{\underline{n} \setminus \text{supp}(c)}$  has rank  $k - 1$ , then any binomial associated to  $c$  is primitive.

**Theorem 3.3.** *Let  $\mathcal{C}$  be a binary  $[n, k]$  code. The universal Gröbner basis for the corresponding code ideal  $I_{\mathcal{C}}$  is given by the set*

$$\mathcal{U}_{\mathcal{C}} = \left\{ \mathbf{x}^c - \mathbf{x}^{c'} \mid c - c' \in \mathcal{C}, \text{wt}(c - c') \leq n - k + 1, \text{rk}(G_{\underline{n} \setminus \text{supp}(c - c')}) = k - 1 \right\} \\ \cup \{x_i^2 - 1 \mid 1 \leq i \leq n\}.$$

*In other words, the universal Gröbner basis for the code ideal consists of all binomials which correspond to codewords that satisfy the Singleton bound and a particular rank condition.*

This result gives rise to a new class of binary linear codes whose codewords which fulfill the Singleton bound also satisfy the rank condition. A binary linear code  $\mathcal{C}$  is called a *Singleton code* if each non-zero codeword  $c$  with Hamming weight  $\leq n - k + 1$  has the property that the submatrix  $G_{\underline{n} \setminus \text{supp}(c)}$  has rank  $k - 1$  for any generator matrix  $G$  for  $\mathcal{C}$ .

Singleton codes are the parity check codes, the MDS codes, the binary Golay code and its parity check extension, the Simplex codes, and the first order Reed-Muller codes and their duals. On the other hand, not all Hamming codes are Singleton.

## References

- [1] W. Adams and P. Lounstau, "An Introduction to Gröbner Bases", American Mathematical Society, 1994
- [2] D. Cox, J. Little and D. O'Shea, "Using Algebraic Geometry", Springer, 1998
- [3] A. Bigatti and L. Robbiano, "Toric Ideals", *Mathematica Contemporanea*, vol. 21, p. 1-25, 2001
- [4] M. Borges-Quintana, M.A. Borges-Trenard, P. Fitzpatrick and E. Martinez-Moro, "Gröbner bases and combinatorics for binary codes", *AAECC*, vol. 19 (5), p. 393-411, 2008
- [5] N. Dück and K.-H. Zimmermann, "A variant of the Gröbner basis algorithm for computing Hilbert bases", *IJPAM*, vol. 81 (1), p. 145-155, 2012
- [6] N. Dück and K.-H. Zimmermann, "Computing generating sets for quaternary codes using Gröbner bases", *IJPAM*, vol. 84 (1), p. 99-109, 2013
- [7] N. Dück and K.-H. Zimmermann, "Universal Gröbner bases for binary linear codes", *IJPAM*, to appear
- [8] M. Kreuzer and L. Robbiano, "Computational Commutative Algebra 2", Springer, 2005
- [9] B. Sturmfels, "Gröbner Bases and Convex Polytopes", American Mathematical Society, 1996
- [10] B. Sturmfels, "Algorithms in Invariant Theory", Springer, 2008

# A Class of Binary Sequences with Large Linear Complexity

Amparo Fúster Sabater  
Security Information Institute, C.S.I.C.  
144 Serrano, 28006 Madrid, Spain

amparo@iec.csic.es

## Abstract

Sequence generators based on Linear Feedback Shift Registers (LFSRs) are very common procedures to generate pseudorandom sequences for multiple applications: computer simulation, circuit testing, error-correcting codes or cryptography (stream ciphers).

The encryption procedure in stream ciphers tries to imitate the mythic *one-time pad cipher* [1] that remains as the only known perfectly secure cipher. This encryption procedure is designed to generate from a short key a long sequence (*keystream sequence*) of seemingly random bits. Some of the most recent designs in stream ciphers can be found in [2]. Typically, a stream cipher consists of a keystream generator whose output sequence is bit-wise XORed with the plaintext (in emission) in order to obtain the ciphertext or with the ciphertext (in reception) in order to recover the original plaintext. References [3, 4] provide a solid introduction to the study of stream ciphers.

Most keystream generators are based on maximal-length LFSRs [6] whose output sequences or *m*-sequences are combined by means of nonlinear filters, nonlinear combiners, irregularly decimated generators, typical elements from block ciphers, etc to produce sequences of cryptographic application.

Desirable properties for such sequences can be enumerated as follows:

1. Long Period
2. Good statistical properties
3. Large Linear Complexity (*LC*).

One general technique for building a keystream generator is to use a nonlinear filter, i.e. a nonlinear function applied to the stages of a single maximal-length LFSR. That is the output sequence is generated as the image of a nonlinear Boolean function *F* in the LFSR stages. Period and statistical properties of the filtered sequences are characteristics deeply studied in the literature, see [7] and the references above mentioned. In addition, such sequences have to pass all 19 DIEHARD tests [8] to be accepted as cryptographic sequences.

Regarding the third requirement, linear complexity of a sequence is defined as the amount of known sequence necessary to reconstruct the entire sequence. In cryptographic terms, *LC* must be as large as possible in order to prevent the application of the Berlekamp-Massey algorithm [9]. A recommended value for *LC* is about half the sequence period. Although several contributions to the linear complexity of nonlinearly filtered sequences can be found in the literature [5], [10] or [11], the problem of determining the exact value of the linear complexity attained by any nonlinear filter is still open.

Now some basic notation is introduced:

*Nonlinear filter.* It is a Boolean function  $F(x_0, x_1, \dots, x_{L-1})$  in *L* variables of degree *k*. For a subset  $A = \{a_0, a_1, \dots, a_{r-1}\}$  of  $\{0, 1, \dots, L-1\}$  with  $r \leq k$ , the notation  $x_A = x_{a_0} x_{a_1} \dots x_{a_{r-1}}$  is used. The Boolean function can be written as:

$$F(x_0, x_1, \dots, x_{L-1}) = \sum_A c_A x_A, \quad (1)$$

where  $c_A \in \{0, 1\}$  and the summation is taken over all subsets *A* of  $\{0, 1, \dots, L-1\}$ .

*Filtered sequence.* The sequence  $\{z_n\}$  is the keystream or output sequence of the nonlinear filter *F* applied to the *L* stages of the LFSR. The keystream bit  $z_n$  is computed by selecting bits from the *m*-sequence  $\{s_n\}$  such that

$$z_n = F(s_n, s_{n+1}, \dots, s_{n+L-1}). \quad (2)$$

Equation (1) describes the Algebraic Normal Form (ANF) of a nonlinear filter *F*. That is the filter is represented as the sum of distinct products in the variables  $(s_n, s_{n+1}, \dots, s_{n+L-1})$ .

The ANF representation of a nonlinear filter is unique. At the same time, a nonlinear filter  $F(s_n, s_{n+1}, \dots, s_{n+L-1})$  can be represented in terms of a  $N$ -tuple of coefficients  $(C_1, C_2, \dots, C_N)$  with  $C_i \in GF(2^L)$  where each coefficient determines the starting point of its corresponding *characteristic sequence* and  $N$  denotes the number of cosets of weight  $\leq k$ , see [5].

In this work, a method of computing all the nonlinear filters of order  $k$  applied to a LFSR with linear complexity  $LC \geq \binom{L}{k}$  (where  $L$  is the LFSR length) has been developed. The procedure is based on the concept of equivalence classes of nonlinear filters and on the handling of such filters from different classes.

Let  $G$  be the set of the  $k$ th-order nonlinear filters applied to a LFSR of length  $L$ . We are going to group the elements of  $G$  producing the filtered sequence  $\{z_n\}$  or a shifted version of such a sequence. Therefore, two different nonlinear filters  $F_0, F_1$  in the same equivalence class will produce shifted versions of the same filtered sequence.

After distinct operations on the nonlinear filters from different equivalence classes, the final result of this computing method is:

1. A set of  $N$  basic filters of the form  $(0, 0, \dots, d_i, \dots, 0, 0)$  ( $1 \leq i \leq N$ ) with  $d_i \in GF(2^L), d_i \neq 0$ .
2. Their corresponding ANF representations.

The combination of all these basic filters with  $d_i$  ( $1 \leq i \leq N$ ) ranging in  $GF(2^L)$  (with their corresponding ANF representations) gives rise to all the possible terms of order  $k$  that preserve the cosets of weight  $k$ . From such terms, all the nonlinear filters of order  $k$  with a guaranteed linear complexity  $LC \geq \binom{L}{k}$  can be constructed. Recall that the construction method involves very simple operations:

- Sum operation: that is reduced to a sum of filters for the ANF representation or to a sum of elements of the extended field  $GF(2^L)$  that expressed in binary representation is just the XOR logic operation.
- Shifting operation through an equivalence class: that means an increment by 1 in all the indexes in the ANF representation.

Consequently, the efficiency of the computation method is quite evident. In brief, we provide one with the complete class of nonlinear filters with  $LC \geq \binom{L}{k}$  at the price of minimal computational operations.

No restriction is imposed on the parameters of the nonlinear filtering function. The method completes the families of nonlinear filters with guaranteed large  $LC$  given in [5].

### Keywords

Pseudorandom sequences, linear complexity, nonlinear filter, cryptography

## References

- [1] N. Nagaraj, One-Time Pad as a nonlinear dynamical system. *Commun Nonlinear Sci Numer Simulat* 17 (2012) 4029-4036.
- [2] eSTREAM, the ECRYPT Stream Cipher Project, The eSTREAM Portfolio in 2012, available at <http://www.ecrypt.eu.org/documents/D.SYM.10-v1.pdf>
- [3] A.J. Menezes *et al.*, Handbook of Applied Cryptography, New York: CRC Press, 1997.
- [4] C. Paar, J. Pelzl, Understanding Cryptography, Springer-Verlag, Berlin Heidelberg, 2010.
- [5] R.A. Rueppel, Analysis and Design of Stream Ciphers, Springer, New York, 1986.
- [6] S. Golomb, Shift-Register Sequences, Aegean Park Press, Laguna Hills, California, 1982.
- [7] A. Fúster-Sabater *et al.*, Deterministic Computation of Pseudorandomness in Cryptographic Sequences. Proc. of ICCS 2009, Part I, LNCS, Vol. 5544, Springer-Verlag, 2009, pp. 621-630.
- [8] A. Marsaglia, Test of DIEHARD, <http://stat.fsu.edu/pub/diehard/>, 1998.
- [9] J.L. Massey, Shift-Register Synthesis and BCH Decoding. *IEEE Trans. Information Theory*, 15(1) (1969) 122-127.
- [10] K. Limniotis, N. Kolokotronis, N. Kalouptsidis, On the Linear Complexity of Sequences Obtained by State Space Generators. *IEEE Trans. Inform. Theory*. 54 (2008) 1786-1793.
- [11] S. Ronjom, C. Cid, Nonlinear Equivalence of Stream Ciphers. Proc. of Fast Software Encryption, FSE 2010, Seoul, Korea, LNCS, Vol. 6147, Springer-Verlag, 2010, pp. 40-54.

# Further Improvements on the Feng-Rao Bound for Dual Codes

Olav Geil, Stefano Martin  
Aalborg University (Denmark)

`stefano@math.aau.dk`

## Abstract

The famous Feng-Rao bound for the minimum distance of dual codes was born using a language close to that of affine variety codes. Afterwards it was generalized to the level of general linear codes. The first generalized version of the Feng-Rao bound used one basis for  $\mathbb{F}_q^n$  and the well-behaving (WB) property. Later formulations use two or three bases of  $\mathbb{F}_q^n$ , the weakly well-behaving (WWB) property or, even, the one-way well-behaving (OWB) property. It is trivial to prove that the Feng-Rao bound obtained with OWB property is at least as sharp as the one obtained with WWB property which in turn is at least as sharp as the one with WB. Whereas it is known that WWB produces sometimes strictly better results than WB, until now no examples have been known for which OWB produces better results than WWB.

In 2006 Salazar, Dunn and Graham proposed the advisory bound based on the WWB property and the analysis of the syndromes of the dual code. This bound was a new improvement of the Feng-Rao bound for the minimum distance, but they still used a language connected with affine variety codes.

We give several contributions.

- We show that the advisory bound can be generalized for general linear code and that this bound is a consequence of a lemma from which further improvements of Feng-Rao bound can be derived using the OWB property.
- We introduce a new bound for the minimum distance of dual codes which is sometimes strictly sharper than the advisory bound and always at least as good. To obtain our result we use a relaxation of the concept of OWB property.
- We show how to obtain new bounds for generalized Hamming weights of dual codes using the advisory bound and the new bound proposed in our work. We remind the reader that generalized Hamming weight is relevant for the analysis of wiretap channels of type II, secret sharing schemes based on error correcting codes and the computation of the trellis complexity of a linear code.
- We compare these bounds to each other in illustrative examples. These examples are obtained by analyzing the codes over optimal generalized  $C_{ab}$  curves over  $\mathbb{F}_q$  ( $C_{ab}$  curves with no assumptions on  $\gcd(a, b)$  and with  $aq$  roots). Furthermore they demonstrate for the first time in the literature that the Feng-Rao bound with OWB can sometimes be strictly sharper than the one equipped with WWB.



In our examples we generate several tables comparing the performances of the bounds.

**Example:**

Consider  $X^4 - Y^6 + X^2 + X - Y^5 - Y^3 \in \mathbb{F}_8[X, Y]$  and the corresponding variety  $\{P_1, \dots, P_{32}\}$ . Let  $\prec_w$  be the weighted degree lexicographic ordering with  $w(X) = 3, w(Y) = 2$  and  $X \succ_{\text{Lex}} Y$ . Consider the footprint  $\Delta_{\prec_w}(\langle X^4 - Y^6 + X^2 + X - Y^5 - Y^3, X^8 - X, Y^8 - Y \rangle) = \{N_1, \dots, N_{32}\}$ ; enumerated with respect to  $\prec_w$ . Write  $\vec{w}_i = (N_i(P_1), \dots, N_i(P_n))$  for  $i = 1, \dots, 32$  and define the dual code  $C(s) = \{\vec{c} \in \mathbb{F}_8^{32} \mid \vec{c} \cdot \vec{w}_1 = \dots = \vec{c} \cdot \vec{w}_s = 0\}$ . We derive the results in Figure 1.

	dimension				$d_1$				$d_2$					
$\gamma^7$	12	7	3	1	$\gamma^7$	$13^5$	$16^1$	$26^2$	$32^1$	$\gamma^7$	$15^1$	$24^2$	$31^1$	—
$\gamma^6$	16	10	5	2	$\gamma^6$	$10^5$	$14^1$	$22^2$	$28^1$	$\gamma^6$	$13^5$	$16^1$	$26^2$	$32^1$
$\gamma^5$	20	14	8	4	$\gamma^5$	$6^1$	$12^4$	$16^1$	$24^1$	$\gamma^5$	$9^4$	$14^1$	$22^2$	$28^1$
$\gamma^4$	24	18	11	6	$\gamma^4$	$4^1$	$8^3$	$14^1$	$20^1$	$\gamma^4$	$6^1$	$12^4$	$16^1$	$24^1$
$\gamma^3$	27	22	15	9	$\gamma^3$	$3^1$	$4^1$	$12^4$	$16^1$	$\gamma^3$	$4^1$	$8^3$	$14^1$	$20^1$
$\gamma^2$	29	25	19	13	$\gamma^2$	$3^1$	$4^1$	$8^3$	$12^4$	$\gamma^2$	$4^1$	$6^1$	$11^4$	$15^1$
$\gamma$	31	28	23	17	$\gamma$	$2^1$	$3^1$	$4^1$	$8^3$	$\gamma$	$3^1$	$4^1$	$7^1$	$12^4$
1	32	30	26	21	1	$1^1$	$2^1$	$3^1$	$4^1$	1	$2^1$	$3^1$	$4^1$	$8^3$
	1	X	$X^2$	$X^3$		1	X	$X^2$	$X^3$		1	X	$X^2$	$X^3$

	$d_3$				$d_4$				$d_5$					
$\gamma^7$	$16^1$	$26^2$	$32^1$	—	$\gamma^7$	$21^1$	$28^1$	—	—	$\gamma^7$	$22^1$	$30^1$	—	—
$\gamma^6$	$14^1$	$22^2$	$28^1$	—	$\gamma^6$	$15^1$	$24^2$	$31^1$	—	$\gamma^6$	$16^1$	$26^1$	$32^1$	—
$\gamma^5$	$12^4$	$15^1$	$24^2$	$31^1$	$\gamma^5$	$13^1$	$16^1$	$26^2$	$32^1$	$\gamma^5$	$14^1$	$21^1$	$28^1$	—
$\gamma^4$	$8^3$	$13^1$	$20^1$	$27^1$	$\gamma^4$	$10^3$	$14^1$	$22^2$	$28^1$	$\gamma^4$	$12^3$	$15^1$	$24^1$	$31^1$
$\gamma^3$	$6^1$	$10^3$	$15^1$	$23^1$	$\gamma^3$	$8^3$	$12^3$	$16^1$	$24^1$	$\gamma^3$	$9^3$	$13^1$	$20^1$	$27^1$
$\gamma^2$	$5^1$	$8^3$	$12^1$	$16^1$	$\gamma^2$	$6^1$	$10^3$	$14^1$	$20^1$	$\gamma^2$	$8^3$	$11^1$	$20^1$	$22^1$
$\gamma$	$4^1$	$6^1$	$8^1$	$14^1$	$\gamma$	$5^1$	$7^1$	$11^1$	$15^1$	$\gamma$	$6^1$	$8^1$	$12^1$	$16^1$
1	$3^1$	$4^1$	$7^1$	$10^3$	1	$4^1$	$6^1$	$8^1$	$12^3$	1	$5^1$	$7^1$	$10^1$	$14^1$
	1	X	$X^2$	$X^3$		1	X	$X^2$	$X^3$		1	X	$X^2$	$X^3$

Figure 1: The figure lists the dimensions of codes  $C(s)$  over  $\mathbb{F}_8$  and corresponding estimates on the generalized Hamming weights  $d_1, \dots, d_5$ . Information about  $C(s)$  is placed in position  $\vec{w}_{s+1}$ . An entry  $z^1$  means that the value  $z$  was obtained from the Feng-Rao bound with WB,  $z^2$  indicates that the same bound with WWB was used, and finally  $z^3$  the same bound with OWB. With  $z^4$  we indicate that the value  $z$  was obtained from the advisory bound and by  $z^5$  that the bound proposed in our work was used.

**Keywords**

Coding Theory, Feng-Rao Bound, Generalized Hamming Weight

# Some Optimal Codes as Tanner Codes with BCH Component Codes

Tom Høholdt, Fernando Piñero

Department of Applied Mathematics and Computer Science - DTU (Denmark)

Peng Zeng

Shanghai Key Laboratory of Trustworthy Computing – ECNU (China)

pzens@sei.ecnu.edu.cn

## Abstract

In this paper we study a class of graph codes with BCH component codes as affine variety codes. We are able to find some optimal binary and ternary codes as Tanner codes with BCH component codes. We choose a special subgraph of the point-line incidence plane of  $\mathbb{P}(2, q)$  as the Tanner graph, and we are able to describe the codes using Gröbner basis.

## Keywords

Tanner Graph, Tanner codes, graph codes, optimal codes

## Introduction

In 1981 Tanner [4] introduced a construction of error-correcting codes based on bipartite graphs. Since then results on their dimension, minimum distance and decoding have been obtained. In this paper we consider some specific bipartite graphs based on finite geometries and codes constructed from these graphs. We use techniques from algebra to compute the dimension when this class of graph codes has BCH component codes. We find some optimal binary and ternary codes in this class of codes.

In this paper  $q$  denotes a power of prime  $p$ ,  $\mathbb{F}_q$  the field with  $q$  elements, and  $[n, k, d]_q$  a code with length  $n$ , dimension  $k$ , and minimum distance  $d$  over  $\mathbb{F}_q$ .

## Tanner Codes and Graph Codes

In this section, we introduce two important codes based on graphs: Tanner Codes and Graph Codes. We also discuss the relations between the two constructions.

**Definition 1** ([4]). *Let  $G$  be an  $(m, n)$ -regular bipartite graph with vertex set  $V = V_1 \cup V_2$ . Let  $N = |V_1|$ . For  $v \in V_2$ , we assume an ordering on the set  $\mathcal{N}(v)$ , the vertices in  $V_1$  adjacent to  $v$ , given by  $\phi_v$ , where  $\phi_v$  is a bijection from  $\{1, 2, \dots, n\}$  to  $\mathcal{N}(v)$ . Furthermore we define  $(c)_{\mathcal{N}(v)} := (c_{\phi_v(1)}, c_{\phi_v(2)}, \dots, c_{\phi_v(n)}) \in \mathbb{F}_q^n$ .*

*Let  $C$  be a code of length  $n$  over  $\mathbb{F}_q$ . We define the Tanner code*

$$(G, C) := \{(c_v) \in \mathbb{F}_q^N \mid \forall v \in V_2 : (c)_{\mathcal{N}(v)} \in C\}.$$

*The vertices of  $V_1$  are known as the variable nodes, as they contain the symbols of the codewords. The vertices of  $V_2$  are known as the constrain nodes, as they represent the parity check equations  $(G, C)$  must satisfy.*

By using a highly structured graph, along with a highly structured code and well-chosen edge labelings, we describe the Tanner code in a nice, algebraic way. The importance of the labeling functions may not be clear from the definition, but the code parameters depend on them. We now define another class of graph based codes. For these codes the labeling functions  $\phi_v$  play a fundamental role as well.

**Definition 2** ([3]). *Let  $G$  be an  $n$ -regular bipartite graph with vertex set  $V = V_1 \cup V_2$  and edge set  $E$  of cardinality  $\#E = N$ . For  $v \in V$ , we assume an ordering on the set  $E(v)$ , the edges incident with  $v$ , given by  $\phi_v$ , where  $\phi_v$  is a bijection from  $\{1, 2, \dots, n\}$  to  $E(v)$ . Furthermore we define  $(c)_{E(v)} := (c_{\phi_v(1)}, c_{\phi_v(2)}, \dots, c_{\phi_v(n)}) \in \mathbb{F}_q^n$ .*

*Let  $C_1$  and  $C_2$  be codes of length  $n$  over  $\mathbb{F}_q$ . We define the graph code*

$$(G, C_1 : C_2) := \{(c_e) \in \mathbb{F}_q^N \mid \forall v \in V_1 : (c)_{E(v)} \in C_1, \forall v \in V_2 : (c)_{E(v)} \in C_2\}.$$

Observe that

$$(G, C_1 : C_2) = (G, C_1 : \mathbb{F}_q^n) \cap (G, \mathbb{F}_q^n : C_2). \quad (1)$$

We define the vertex-edge incidence graph of  $G$ , which illustrates the close connection between Tanner codes and Graph codes.

**Definition 3.** *Let  $G = (V(G), E(G))$  be a graph. We define the vertex-edge adjacency graph of  $G$  as the bipartite graph  $G_{ve} = (V(G) \cup E(G), E)$ . There is an edge of the graph  $G_{ve}$  between the vertex  $v$  of  $G$  and the edge  $e$  of  $G$  if and only if the vertex  $v$  is incident to the edge  $e$  in the graph  $G$ .  $G_{ve}$  has no other edges.*

Now we state the close relation between Tanner Codes and Graph Codes.

**Theorem 1.** *Let  $G$  be an  $n$ -regular bipartite graph. Let  $C$  be a code of length  $n$ , then*

$$(G, [n, 1, n]_q : C) \text{ is an } n\text{-fold repetition of the code } (G, C) \text{ and } (G, C : C) = (G_{ve}, C).$$

*as long as the labelings are consistent.*

*Proof.* The equality  $(G, C : C) = (G_{ve}, C)$  follows from the correspondence between the edges of  $G$  and the vertices of  $G_{ve}$ . The equivalence between  $(G, [n, 1, n] : C)$  and  $(G, C)$  follows from the fact that since all edges incident to a vertex of  $V_1$  must have the same value, we can assign this value to the vertex itself, which is the assignment for the code  $(G, C)$ .  $\square$

We finish this section with some theorems on the dimension of Graph codes.

**Theorem 2.** *Let  $G$  be an  $n$ -regular bipartite graph with  $N$  edges. Let  $C_1, C_2$  be codes of length  $n$  over  $\mathbb{F}_q$  of dimensions  $k_1$  and  $k_2$  respectively. Then*

$$\dim (G, C_1 : C_2) = \frac{N}{n}(k_1 + k_2 - n) + \dim (G, C_1^\perp : C_2^\perp).$$

*Proof.* Assume  $G$  has vertex set  $V = V_1 \cup V_2$ . For each vertex  $v \in V_1$  we get  $k_1$  independent parity check equations for  $C_1^\perp$  involving the edges in  $E(v)$  only. The resulting  $Nk_1/n$  parity check equations of a code of the form  $(G, C_1 : \mathbb{F}_q^n)$  are independent because the edge sets  $E(v)$  and  $E(u)$  are disjoint for  $u \neq v$ . Therefore the dimension of the code  $(G, C_1^\perp : \mathbb{F}_q^n)$  is  $N(n - k_1)/n$ . Similarly, the code  $(G, \mathbb{F}_q^n : C_2^\perp)$  has dimension  $N(n - k_2)/n$ . The parity check equations which are not independent are those corresponding to  $(G, C_1^\perp : \mathbb{F}_q^n) \cap (G, \mathbb{F}_q^n : C_2^\perp)$  which are the codewords of  $(G, C_1^\perp : C_2^\perp)$ .  $\square$

The graph based codes in this paper are defined with the following graph.

**Definition 4.** We define the bipartite graph  $\Gamma := (V_1 \cup V_2, E)$  by:

$$V_1 := \{(x, y) \mid x \in \mathbb{F}_q^*, y \in \mathbb{F}_q\}, \quad V_2 := \{(a, b) \mid a \in \mathbb{F}_q^*, b \in \mathbb{F}_q\}$$

$$\text{and } E := \{((x, y), (a, b)) \in V_1 \times V_2 \mid ax + b - y = 0\}.$$

Note that  $\Gamma$  is a subgraph of the point line incidence graph of the projective plane over  $\mathbb{F}_q$ . Furthermore  $\Gamma$  is  $q - 1$ -regular and it has a nice algebraic description.

**Affine Variety Codes** We start this section with a review of material in [2] and [1]. Let  $\mathbb{F}_q[X_1, \dots, X_m]$  be the polynomial ring in  $m$  variables over  $\mathbb{F}_q$  and  $\mathcal{P} = \{P_1, P_2, \dots, P_N\} \subset \mathbb{F}_q^m$  be a set of  $N$  points in  $\mathbb{F}_q^m$ . Denote by  $\mathbf{I}(\mathcal{P})$  the ideal in  $\mathbb{F}_q[X_1, \dots, X_m]$  consisting of the polynomials which vanish at all points of  $\mathcal{P}$ . We define  $R := \mathbb{F}_q[X_1, \dots, X_m]/\mathbf{I}(\mathcal{P})$  and the evaluation map,

$$Ev_{\mathcal{P}} : R \rightarrow \mathbb{F}_q^N; \quad f \mapsto (f(P_1), f(P_2), \dots, f(P_N)).$$

The map  $Ev_{\mathcal{P}}$  is an isomorphism of vector spaces. Note that in this paper, we often denote an element  $\bar{f} = f + \mathbf{I}(\mathcal{P}) \in R$  by  $f$  for simplicity.

**Definition 5.** Let  $L$  be an  $\mathbb{F}_q$ -linear subspace of  $R$ . We define the affine variety code  $C(\mathbf{I}(\mathcal{P}), L) := Ev_{\mathcal{P}}(L)$ .

Since  $L$  is an  $\mathbb{F}_q$ -linear subspace of  $R$  and  $Ev_{\mathcal{P}}$  is an isomorphism, we have that

$$\dim C(\mathbf{I}(\mathcal{P}), L) = \dim L. \quad (2)$$

**Lemma 1.** Let  $\mathcal{P} \subset \mathbb{F}_q^m$ ,  $R = \mathbb{F}_q[X_1, X_2, \dots, X_m]/\mathbf{I}(\mathcal{P})$  as before. Suppose that  $L$  and  $M$  are two  $\mathbb{F}_q$ -linear subspaces of  $R$ . Then  $C(\mathbf{I}(\mathcal{P}), L) \cap C(\mathbf{I}(\mathcal{P}), M) = C(\mathbf{I}(\mathcal{P}), L \cap M)$ .

*Proof.* If  $c \in C(\mathbf{I}(\mathcal{P}), L) \cap C(\mathbf{I}(\mathcal{P}), M)$ , then  $f \in L$  and  $g \in M$  exist such that  $Ev_{\mathcal{P}}(f) = c = Ev_{\mathcal{P}}(g)$ . Since  $Ev_{\mathcal{P}}$  is injective, then  $f = g$  and therefore that  $f \in L \cap M$ . Therefore  $c \in C(\mathbf{I}(\mathcal{P}), L \cap M)$ . The inclusion  $C(\mathbf{I}(\mathcal{P}), L) \cap C(\mathbf{I}(\mathcal{P}), M) \supseteq C(\mathbf{I}(\mathcal{P}), L \cap M)$  is clear.  $\square$

Since the quotient ring  $R$  plays a fundamental role on Affine Variety codes, the following theorem on an ideal  $\mathbf{I}(\mathcal{P})$  and its quotient ring  $R$  will help our computations with  $R$ .

**Theorem 3** ([1]). Let  $\mathbf{I}(\mathcal{P})$  be an ideal of  $\mathbb{F}_q[X_1, \dots, X_m]$  and  $R = \mathbb{F}_q[X_1, \dots, X_m]/\mathbf{I}(\mathcal{P})$  be the quotient ring of  $R$ . Let  $\delta$  be a monomial ordering, and suppose  $\{g_1, g_2, \dots, g_{m'}\}$  is a Gröbner basis for  $\mathbf{I}(\mathcal{P})$  under  $\delta$  and let  $\Delta_{\delta}$  be the set of monomials which are not divisible by the leading terms of the  $g_i$  under  $\delta$ . Then the following are true:

- $\Delta_{\delta}$ , also known as the footprint of  $\mathbf{I}(\mathcal{P})$  under  $\delta$ , is a  $\mathbb{F}_q$ -linear basis for  $R$ .
- The representation of  $f \in R$  over  $\Delta_{\delta}$  is  $f \bmod \{g_1, g_2, \dots, g_{m'}\}$ .

BCH codes are an example of affine variety codes with  $m = 1$  and  $\mathcal{P} = \{\alpha_1, \alpha_2, \dots, \alpha_{q-1}\} = \mathbb{F}_q^*$ . Then  $\mathbf{I}(\mathcal{P}) = \langle X_1^{q-1} - 1 \rangle$ . BCH codes have several definitions; we use the following. Let  $q$  be a power of  $p$ . Let  $J \subseteq \mathbb{Z}_{q-1}$ , such that  $J$  is closed under multiplication by  $p$  modulo  $q - 1$ . We define  $M(J) := \langle \{X_1^j \mid j \in J\} \rangle_{\mathbb{F}_q}$  of  $R = \mathbb{F}_q[X_1]/\mathbf{I}(\mathcal{P})$ . The BCH code is the affine variety code  $C(\mathbf{I}(\mathcal{P}), M(J))$ . The  $i$ -th coordinate of  $Ev_{\mathcal{P}}(f)$  is  $f(\alpha_i)$ . Furthermore if we define  $\bar{J} = \{q - 1 - j \bmod (q - 1) \mid j \in J\}$  for  $J \subset \mathbb{Z}_{q-1}$ , then  $C(\mathbf{I}(\mathcal{P}), M(J))^{\perp} = C(\mathbf{I}(\mathcal{P}), M(\mathbb{Z}_{q-1} \setminus \bar{J}))$ . The theory of subfield subcodes ensures that this definition is equivalent to the standard definitions of BCH codes.

Now we describe Graph codes over  $\Gamma$  as Affine Variety codes. Since a Graph code over  $G$  assigns a symbol from  $\mathbb{F}_q$  to each edge in  $E(G)$ , we must associate a polynomial ideal  $I(\Gamma)$  to the edge set  $E = E(\Gamma)$ . To do this, let  $\delta_1$  denote the lexicographical order with  $B > A > X > Y$  and  $\delta_2$  denote the lexicographical order with  $Y > X > A > B$ , we have the following theorem for the ideal  $\mathbf{I}(\Gamma) := \langle AX + B - Y, X^{q-1} - 1, Y^q - Y, A^{q-1} - 1, B^q - B \rangle$ .

**Theorem 4.** *The set  $\{AX + B - Y, X^{q-1} - 1, Y^q - Y, A^{q-1} - 1, B^q - B\}$  is a Gröbner basis for  $\mathbf{I}(\Gamma)$  under  $\delta_1$  and  $\delta_2$ .*

*Proof.* The polynomial  $B^q - B$  is a combination of the other four polynomials,  $AX + B - Y, X^{q-1} - 1, Y^q - Y, A^{q-1} - 1$ . As no leading term under  $\delta_1$  of this basis for  $\mathbf{I}(\Gamma)$  contains any common factor with another leading term, these four polynomials constitute a Gröbner basis for  $\mathbf{I}(\Gamma)$ . The proof for  $\delta_2$  is similar.  $\square$

Denote by  $\Delta_1$  the footprint of  $\mathbf{I}(\Gamma)$  under  $\delta_1$  and by  $\Delta_2$  the footprint of  $\mathbf{I}(\Gamma)$  under  $\delta_2$ .

**Theorem 5.** *The ideal  $\mathbf{I}(\Gamma)$  is the ideal of  $E$ , the edge set of  $\Gamma$ .*

*Proof.* The elements of  $\mathbf{I}(\Gamma)$  vanish at all the points of  $E$ . Therefore  $\mathbf{I}(\Gamma) \subset \mathbf{I}(E)$ . This implies that  $\dim \mathbb{F}_q[X, Y, A, B]/\mathbf{I}(\Gamma) \geq \dim \mathbb{F}_q[X, Y, A, B]/\mathbf{I}(E) = \#E = q(q-1)^2$ . Since  $\#\Delta_1 = q(q-1)^2$ , then  $\dim \mathbb{F}_q[X, Y, A, B]/\mathbf{I}(\Gamma) = q(q-1)^2$ , which implies  $\mathbf{I}(\Gamma) = \mathbf{I}(E)$   $\square$

We need a vertexwise edge labeling of the edges of  $\Gamma$ . The labelings we will use are:

$$\phi_{(x,y)}(i) := (x, y, \alpha_i, y - x\alpha_i), \quad (x, y) \in V_1, \quad \text{and} \quad \phi_{(a,b)}(i) := (\alpha_i, a\alpha_i + b, a, b), \quad (a, b) \in V_2.$$

For any  $J \subset \mathbb{Z}_{q-1}$ , we describe the codes  $(\Gamma, C(\mathbf{I}(\mathcal{P}), M(J)) : \mathbb{F}_q^{q-1})$  and  $(\Gamma, \mathbb{F}_q^{q-1} : C(\mathbf{I}(\mathcal{P}), M(J)))$  as affine variety codes.

**Definition 6.** *Let  $J \subset \mathbb{Z}_{q-1}$  and  $R = \mathbb{F}_q[X, Y, A, B]/\mathbf{I}(\Gamma)$ , we define*

$$L_1(J) := \langle \{X^{i_1} Y^{i_2} A^{j_1} \mid j_1 \in J\} \rangle_{\mathbb{F}_q} \subset R, \quad \text{and} \quad L_2(J) := \langle \{A^{j_1} B^{j_2} X^{i_1} \mid i_1 \in J\} \rangle_{\mathbb{F}_q} \subset R.$$

Note that the elements of  $L_1(J)$  and  $L_2(J)$  belong to the quotient ring  $R$ . In particular the monomials in the above definition may not be linearly independent, because we are working modulo  $\mathbf{I}(\Gamma)$ . We use the representations of  $L_1(J_X)$  and  $L_2(J_A)$  under  $\Delta_1$  and  $\Delta_2$  to describe the graph code  $(\Gamma, C(\mathbf{I}(\mathcal{P}), M(J_X)) : C(\mathbf{I}(\mathcal{P}), M(J_A)))$  as an affine variety code. By Eq. (1) we have the equality  $(\Gamma, C(\mathbf{I}(\mathcal{P}), M(J_X)) : C(\mathbf{I}(\mathcal{P}), M(J_A))) = (\Gamma, C(\mathbf{I}(\mathcal{P}), M(J_X)) : \mathbb{F}_q^{q-1}) \cap (\Gamma, \mathbb{F}_q^{q-1} : C(\mathbf{I}(\mathcal{P}), M(J_A)))$ .

**Theorem 6.** *We have*

$$C(\mathbf{I}(\Gamma), L_1(J_X)) = (\Gamma, C(\mathbf{I}(\mathcal{P}), M(J_X)) : \mathbb{F}_q^{q-1})$$

$$\text{and } C(\mathbf{I}(\Gamma), L_2(J_A)) = (\Gamma, \mathbb{F}_q^{q-1} : C(\mathbf{I}(\mathcal{P}), M(J_A))).$$

$$\text{Moreover, } (\Gamma, C(\mathbf{I}(\mathcal{P}), M(J_X)) : C(\mathbf{I}(\mathcal{P}), M(J_A))) = C(\mathbf{I}(\Gamma), L_1(J_X) \cap L_2(J_A)).$$

*Proof.* Let  $f(X, Y, A, B) \in L_1(J_X)$  and  $c = (f(x, y, a, b))_{(x,y,a,b) \in E}$ . For  $(x, y) \in V_1$ , the univariate polynomial  $p(A) := f(x, y, A, y - Ax)$  is in the vector space  $\langle \{A^j \mid j \in J_X\} \rangle_{\mathbb{F}_q}$  since the coefficients where  $y - Ax$  is raised to a nonzero power are zero. Therefore the codeword  $(p(\alpha_1), p(\alpha_2), \dots, p(\alpha_{q-1}))$  is a codeword in  $C(\mathbf{I}(\mathcal{P}), M(J_X))$ . On the other hand  $(c)_{E((x,y))} = (f(x, y, \alpha_1, y - \alpha_1 x), \dots, f(x, y, \alpha_{q-1}, y - \alpha_{q-1} x))$ . We see that the value of the polynomial  $p(A)$  at  $A = \alpha_i$  is equal to the  $i$ -th coordinate of  $(c)_{E((x,y))}$ . Therefore  $c \in (\Gamma, C(\mathbf{I}(\mathcal{P}), M(J_X)) : \mathbb{F}_q^{q-1})$  implying  $C(\mathbf{I}(\Gamma), L_1(J_X)) \subset (\Gamma, C(\mathbf{I}(\mathcal{P}), M(J_X)) : \mathbb{F}_q^{q-1})$ .

By the reasoning in the proof of Theorem 2, we obtain  $\dim(\Gamma, C(\mathbf{I}(\mathcal{P}), M(J_X)) : \mathbb{F}_q^{q-1}) = q(q-1)|J_X|$ . Since the elements of  $L_1(J_X) \cap \Delta_1$  are linearly independent, the inequality  $\dim L_1(J_X) \geq q(q-1)|J_X| = |L_1(J_X) \cap \Delta_1|$  follows easily. Equation (2), implies  $C(\mathbf{I}(\Gamma), L_1(J_X)) = (\Gamma, C(\mathbf{I}(\mathcal{P}), M(J_X)) : \mathbb{F}_q^{q-1})$ . Similarly  $C(\mathbf{I}(\Gamma), L_2(J_A)) = (\Gamma, \mathbb{F}_q^{q-1} : C(\mathbf{I}(\mathcal{P}), M(J_A)))$  holds. The final statement follows from the above and Lemma 1.  $\square$

The dimension of  $(\Gamma, C(\mathbf{I}(\mathcal{P}), M(J_X)) : C(\mathbf{I}(\mathcal{P}), M(J_A)))$  equals the dimension of the  $\mathbb{F}_q$ -linear subspace  $\langle L_1(J_X) \rangle_{\mathbb{F}_q} \cap \langle L_2(J_A) \rangle_{\mathbb{F}_q}$  of  $R$ . Although  $L_1(J_X) \cap \Delta_1$  is a basis for  $\langle L_1(J_X) \rangle_{\mathbb{F}_q}$  and  $L_2(J_A) \cap \Delta_2$  is a basis for  $\langle L_2(J_A) \rangle_{\mathbb{F}_q}$ , their intersection is hard to compute. Since the Gröbner basis for  $I(\Gamma)$  under  $\delta_1$  is nice, the remainder of  $f \in \langle \Delta_2 \rangle$  over the basis  $\Delta_1$  is also nice, which implies the change of basis matrix from  $\Delta_2$  to  $\Delta_1$  is quite nice.

**Theorem 7.** Let  $U_q = ((\binom{j}{i}))_{0 \leq i, j < q}$  be the upper triangular Pascal matrix of binomial coefficients in  $\mathbb{F}_p$ . Then the change of basis matrix from  $\Delta_1$  to in  $\Delta_2$  is a permutation of a block diagonal  $q(q-1)^2 \times q(q-1)^2$  matrix with  $(q-1)^2$  blocks of the matrix  $U_q$ .

*Proof.* Fix  $0 \leq i_1, j_1 < q-1$ . A monomial of the form  $X^{i_1-l} A^{j_1-l} Y^l$ , where the powers  $i_1-l$  and  $j_1-l$  are taken mod  $q-1$  is mapped to  $\sum_{m=0}^l \binom{l}{m} B^m A^{j_1-m} X^{i_1-m}$ . Therefore a polynomial in  $\langle X^{i_1-l} A^{j_1-l} Y^l \rangle_{\mathbb{F}_q}$  is mapped to a polynomial in  $\langle X^{i_1-l} A^{j_1-l} B^l \rangle_{\mathbb{F}_q}$  according to the Pascal matrix  $U_q$ .  $\square$

With this simpler basis, we can easily compute the dimension of the  $\mathbb{F}_q$ -linear space  $L_1(\{0\}) \cap L_2(J_A)$ . We present some optimal codes we have found in this manner.

#### Optimal Codes

We have found some optimal binary and ternary codes as Tanner codes of the graph  $\Gamma$  with the BCH component codes described in the following table.

$q$	$J_A$	$(\Gamma, C(\mathbf{I}(\mathcal{P}), M(J_A)))$	Status
8	{1, 2, 4}	[56, 6, 28] <sub>2</sub>	Optimal
	{0, 1, 2, 4}	[56, 10, 24] <sub>2</sub>	Optimal
16	{5, 10}	[240, 2, 160] <sub>2</sub>	Optimal
	{1, 2, 4, 8}	[240, 8, 120] <sub>2</sub>	Optimal
	{0, 1, 2, 4, 8}	[240, 13, 112] <sub>2</sub>	Best Known
9	{1, 3}	[72, 2, 54] <sub>3</sub>	Optimal
	{0, 1, 3}	[72, 5, 45] <sub>3</sub>	Best Known

**Acknowledgment** The authors gratefully acknowledge the support from the Danish National Research Foundation and the National Science Foundation of China (Grant No.11061130539) for the Danish-Chinese Center for Applications of Algebraic Geometry in Coding Theory and Cryptography. The third author would also like to acknowledge the support of the National Natural Science Foundation of China under Grants No. 61021004 and 61103222 and the Research Fund for the Doctoral Program of Higher Education of China under grant No. 20110076120016.

## References

- [1] David Cox, John Little, and Donal O’Shea. *Ideals, Varieties and Algorithms*. Springer, 2007.
- [2] J. Fitzgerald and R.F. Lax. Decoding affine variety codes using gröbner bases. *DCC*, 13:147–158, 1998.
- [3] Ron M. Roth. *Introduction to Coding Theory*. Cambridge University Press, 2006.
- [4] R. Tanner. A recursive approach to low complexity codes. *IEEE Trans. Inf. Theory*, 27(5):533 – 547, sep 1981.

# A secret sharing scheme using Gröbner basis

Hiroshi Kai and Masaki Yamada  
Graduate School of Science and Engineering, Ehime University (Japan)

{kai, yamada.m}@hpc.cs.ehime-u.ac.jp

## Abstract

A secret sharing scheme will be proposed by a computer algebra algorithm. Wang et al. have already proposed a secret sharing scheme using Gröbner basis. We will show another one using Gröbner basis. Our method reduces required memory space to hold share information for participants.

## Keywords

Secret sharing scheme, Gröbner basis, Cheater detection

## 1 Introduction

The secret sharing scheme was proposed by Shamir [1] and Blakley [2] independently. In the scheme, a secret  $s \in Z_p$  where  $p$  is a prime number is divided into  $n$  shares. The  $n$  shares are held by  $n$  different participants respectively. If we have  $k$  shares, where  $k \leq n$ , then the secret can be easily computed from them. However, we know only  $l$  shares, where  $l < k$ , then the secret never be obtained. The above scheme is called as  $(k, n)$  secret sharing scheme.

It is well known that there are a lot of methods to realize the  $(k, n)$  secret sharing scheme. In this paper, we consider a secret sharing scheme based on a computer algebra algorithm. Wang, et al. [3] have already proposed a secret sharing scheme using Gröbner basis. In the method, shares are presented by  $n + 1$  multivariate polynomials. In this paper, we propose another method using Gröbner basis. In our method, shares are presented by  $n$  polynomials, and the memory space to hold the share information for participants may be reduced.

## 2 A secret sharing scheme by Wang et al.

Let  $F$  be a field and  $F[x_1, x_2, \dots, x_m]$  be a polynomial ring. We take a secret  $s \in F$ . Then, their scheme is described as follows.

- 1 A dealer chooses  $k$  random polynomials  $f_1, \dots, f_k \in F[x_1, x_2, \dots, x_m]$ .
- 2 The dealer chooses a random matrix  $B \in F^{n \times k}$ . Then  $(g_1, \dots, g_n)^T = B \times (f_1, \dots, f_k)^T$ .
- 3 The dealer chooses a polynomial  $g = s + a_1 f_1 + \dots + a_k f_k$ , where  $a_i \in F, i = 1, \dots, k$  are random numbers. The dealer announces the share information  $(g_i, g)$  to a participant  $P_i$  for  $i = 1, \dots, k$ .

If we obtain  $k$  shares  $g_{i_1}, g_{i_2}, \dots, g_{i_k}$  among the  $n$  shares, then the secret  $s$  can be computed from the polynomial  $g$  and Gröbner basis of  $\langle g_{i_1}, g_{i_2}, \dots, g_{i_k} \rangle$ .

Note that the scheme must satisfy following two conditions:

- 1  $f_1, \dots, f_k \in \langle g_{i_1}, \dots, g_{i_k} \rangle$  and  $g_{i_j} \notin \langle g_{i_1}, \dots, g_{i_{j-1}}, g_{i_{j+1}}, \dots, g_{i_k} \rangle$ .
- 2 For any submatrix  $B_1 \in F^{k \times k}$  of  $B$ ,  $(b_1, \dots, b_k) = (a_1, \dots, a_k) \times B_1^{-1}$ . Then,  $b_i \neq 0$  for all  $i$ .

They showed that, if these conditions are true, then the scheme is a  $(k, n)$  secret sharing scheme.

### 3 Proposed method

In this paper, we consider another scheme as follows.

- 1 A dealer chooses  $k - 1$  random polynomials  $f_1, \dots, f_{k-1} \in F[x_1, x_2, \dots, x_m]$ .
- 2 The dealer chooses a random matrix  $B \in F^{n \times k-1}$ . Then  $(g_1, \dots, g_n)^T = s(1, 1, \dots, 1)^T + B \times (f_1, \dots, f_{k-1})^T$
- 3 The dealer announces the share information  $g_i$  to a participant  $P_i$ .

For  $i \neq j$ , we define  $g_{i,j} = g_i - g_j$ , where note that  $g_{i,j} \in \langle f_1, \dots, f_{k-1} \rangle$ . If we obtain  $k$  shares  $g_{i_1}, \dots, g_{i_k}$ , then we can compute  $k - 1$  polynomials  $g_{i_1, i_2}, g_{i_2, i_3}, \dots, g_{i_{k-1}, i_k}$ . The secret  $s$  will be found from  $g_i$  and Gröbner basis of  $\langle g_{i_1, i_2}, g_{i_2, i_3}, \dots, g_{i_{k-1}, i_k} \rangle$ .

In the scheme, participant  $P_i$  hold only a polynomial  $g_i$ , while participants in the scheme proposed by Wang et al have to keep two polynomials.

However, the following condition must be true to be a  $(k, n)$  secret sharing scheme.

- 1  $f_1, \dots, f_k \in \langle g_{i_1, i_2}, \dots, g_{i_{k-1}, i_k} \rangle$  and  $g_{i_{j-1}, i_j} \notin \langle g_{i_1, i_2}, \dots, g_{i_{j-2}, i_{j-1}}, g_{i_j, i_{j+1}}, \dots, g_{i_{k-1}, i_k} \rangle$ .
- 2 Let  $B_1$  and  $B_2$  be  $(k - 1) \times (k - 1)$  submatrices of  $B$  as follows.

$$B_1 = \begin{pmatrix} b_{j_1,1} & b_{j_1,2} & \cdots & b_{j_1,k-1} \\ b_{j_2,1} & b_{j_2,2} & \cdots & b_{j_2,k-1} \\ \vdots & \vdots & & \vdots \\ b_{j_{k-1},1} & b_{j_{k-1},2} & \cdots & b_{j_{k-1},k-1} \end{pmatrix}$$

$$B_2 = \begin{pmatrix} b_{j_2,1} & b_{j_2,2} & \cdots & b_{j_2,k-1} \\ b_{j_3,1} & b_{j_3,2} & \cdots & b_{j_3,k-1} \\ \vdots & \vdots & & \vdots \\ b_{j_k,1} & b_{j_k,2} & \cdots & b_{j_k,k-1} \end{pmatrix}$$

Then,  $c_{i,j} \neq 0$ , where

$$\begin{pmatrix} c_{1,1} & c_{1,2} & \cdots & c_{1,k-1} \\ c_{2,1} & c_{2,2} & \cdots & c_{2,k-1} \\ \vdots & \vdots & & \vdots \\ c_{k,1} & c_{k,2} & \cdots & c_{k,k-1} \end{pmatrix} = \begin{pmatrix} b_{j_1,1} & b_{j_1,2} & \cdots & b_{j_1,k-1} \\ b_{j_2,1} & b_{j_2,2} & \cdots & b_{j_2,k-1} \\ \vdots & \vdots & & \vdots \\ b_{j_k,1} & b_{j_k,2} & \cdots & b_{j_k,k-1} \end{pmatrix} \times (B_1 - B_2)^{-1}$$

We can prove, analogously to the proof of Theorem 2.1 [3], that the proposed scheme is a  $(k, n)$  secret sharing scheme, if the above conditions are true.

Further, as mentioned in [3], the scheme may be applied to cheater detection, because  $s$  may be recovered as a polynomial (not a number, with high probability), if a participant gives an incorrect share.

### 4 Conclusions

We proposed a secret sharing scheme by Gröbner basis. In the scheme, share information is presented by a multivariate polynomial. Under the conditions described above, the scheme is a  $(k, n)$  secret sharing scheme. It is important to estimate how much computation time is required, and to consider how we can identify a wrong share if there is a cheater among the participants, but they remain future works.

### References

- [1] Adi Shamir, How to Share a Secret, Communications of the ACM, Vol.22, Issue 11, pp.612-613, 1979.
- [2] George R. Blakley, Safeguarding cryptographic keys, Proceedings of the National Computer Conference, Vol. 48, pp.313-317, 1979.
- [3] Wang Mingsheng, Feng Dengguo and Wang Guilin, Secret Sharing Schemes Based on Computer Algebra, Journal of Software, Vol. 13, pp.143-148, 2002.



# Error-correcting pairs and arrays from algebraic geometry codes

Irene Márquez-Corbella and Ruud Pellikaan

Dept. of Algebra, Geometry and Topology, University of Valladolid

Facultad de Ciencias, 47005 Valladolid, Spain. E-mail: [imarquez@agt.uva.es](mailto:imarquez@agt.uva.es)

Dept. of Mathematics and Computing Science, Eindhoven University of Techn.

P.O. Box 513, 5600 MB Eindhoven, The Netherlands. E-mail: [g.r.pellikaan@tue.nl](mailto:g.r.pellikaan@tue.nl)

## Abstract

The security of the most popular number-theory public key crypto (PKC) systems will be devastatingly affected by the success of a large quantum computer. Code-based cryptography is one of the promising alternatives that are believed to resist classical and quantum computer attacks. Many families of codes have been proposed for these cryptosystems, one of the main requirements is having an efficient  $t$ -bounded decoding algorithm.

In [16, 17] it was shown that for the so called very strong algebraic geometry codes  $\mathcal{C}$  which is a collection of codes  $C = C_L(\mathcal{X}, \mathcal{P}, E)$ , where  $\mathcal{X}$  is an algebraic curve over  $\mathbb{F}_q$ ,  $\mathcal{P}$  is an  $n$ -tuple of mutually distinct  $\mathbb{F}_q$ -rational points of  $\mathcal{X}$  and  $E$  is a divisor of  $\mathcal{X}$  with disjoint support from  $\mathcal{P}$ , an equivalent representation can be found. Moreover in [19] an efficient computational approach is given to retrieve a triple that is isomorphic with the original representation, and, from this representation, an efficient decoding algorithm is obtained.

In this talk, we will show how an efficient decoding algorithm can be retrieved from an algebraic geometry code  $\mathcal{C}$  by means of error-correcting pairs [20] and arrays directly, that is without the detour via the representation  $(\mathcal{X}, \mathcal{P}, E)$  of the code  $C = C_L(\mathcal{X}, \mathcal{P}, E)$ .

As a consequence we will have that algebraic geometry codes with certain parameters are not secure for the code-based McEliece public key cryptosystem.

## Keywords

Code based cryptography, McEliece public key cryptosystem,  
algebraic geometry codes, error-correcting pairs and arrays.

## 1 Introduction

The security of code-based cryptosystems is founded on the (supposedly) hardness of decoding up to half the minimum distance. The minimum distance decoding problem was shown by Berlekamp-McEliece-Van Tilborg [1, 3] to be NP-hard. McEliece [21] proposed a PKC system using binary Goppa codes.

All known minimum distance decoding algorithms for general codes have exponential complexity in the length of the code. The complexity exponent of decoding general binary codes up to half the minimum distance has been lowered in a series of papers from above  $1/3$  for brute force decoding to below  $1/20$  by [2]. However there are several classes of codes such as the generalized Reed-Solomon (GRS), BCH, Goppa or algebraic geometry codes which have polynomial decoding algorithms that correct up to a certain bound which is at most half the minimum distance.

In 1986 [23] Niederreiter presented a dual version of McEliece cryptosystem which is equivalent in terms of security. This system differs from McEliece's system since it uses a parity check matrix instead of a generator matrix of the code. Several classes of codes are proposed for code-base PKC systems such as subcodes of GRS codes, alternant codes which contains the Goppa codes as subclass, and algebraic geometry codes [12].

It was shown in [6, 14, 24, 26, 28] that the known efficient bounded distance decoding algorithms of the before mentioned codes can be described by a basic algorithm using an error-correcting pair. That means that the proposed McEliece cryptosystem that use these classes of codes can be viewed as using the error-correcting pair as a secret key. Hence the security of these PKC systems is not only based on the inherent intractability of bounded distance decoding but also on the assumption that it is difficult to retrieve an error-correcting pair.

## 2 Error-correcting pairs and arrays

From now on the dimension of a linear code  $C$  will be denoted by  $k(C)$  and its minimum distance by  $d(C)$ . Given two elements  $\mathbf{a}$  and  $\mathbf{b}$  in  $\mathbb{F}_q^n$ , the *star multiplication* is defined by coordinatewise multiplication, that is  $\mathbf{a} * \mathbf{b} = (a_1b_1, \dots, a_nb_n)$  while the *standard inner multiplication* is defined by  $\mathbf{a} \cdot \mathbf{b} = \sum_{i=1}^n a_ib_i$ . In general, for two subsets  $A$  and  $B$  of  $\mathbb{F}_q^n$  the set  $A * B$  is given by  $\{\mathbf{a} * \mathbf{b} \mid \mathbf{a} \in A \text{ and } \mathbf{b} \in B\}$ . Furthermore  $A \perp B$  if and only if  $\mathbf{a} \cdot \mathbf{b} = 0$  for all  $\mathbf{a} \in A$  and  $\mathbf{b} \in B$ .

Let  $C$  be a linear code in  $\mathbb{F}_q^n$ . The pair  $(A, B)$  of linear codes over  $\mathbb{F}_{q^e}$  of length  $n$  is called a *t-error-correcting pair* (ECP) for  $C$  if the following properties hold:

- E.1  $(A * B) \perp C$ ,
- E.2  $k(A) > t$ ,
- E.3  $d(B^\perp) > t$ ,
- E.4  $d(A) + d(C) > n$ .

The notion of an error-correcting pair for a linear code was introduced in 1988 by Pellikaan [24, 26] and independently by Kötter in [14, 15] in 1992. It is shown that a linear code in  $\mathbb{F}_q^n$  with a  $t$ -error-correcting pair has a decoding algorithm which corrects up to  $t$  errors with complexity  $\mathcal{O}((en)^3)$ .

The existence of ECP's for GRS and algebraic geometry codes was shown in [24, 26]. For many cyclic codes Duursma and Kötter in [6, 14, 15] have found ECP's which correct beyond the designed BCH capacity.

An *error-correcting array* is defined in [13, 27] for a sequence of codes. From it follows the *Feng-Rao designed minimum distance* of the codes and the majority voting scheme of Feng-Rao [4, 5, 8] gives a decoding algorithm that decodes these codes up to half the Feng-Rao designed minimum distance with complexity  $\mathcal{O}(n^3)$ . An equivalent formulation is given in terms of (*weakly*) *well-behaving sequences* [9, 10, 11].

## 3 Algebraic geometry codes

Let  $\mathcal{X}$  be an algebraic curve defined over  $\mathbb{F}_q$  with genus  $g$ . Let  $\mathcal{P}$  be an  $n$ -tuple of  $\mathbb{F}_q$ -rational points on  $\mathcal{X}$  and let  $E$  be a divisor of  $\mathcal{X}$  with disjoint support from  $\mathcal{P}$  of degree  $m$ . Then the algebraic geometry code  $C_L(\mathcal{X}, \mathcal{P}, E)$  is the image of the Riemann-Roch space  $L(E)$  of rational functions with prescribed behavior of zeros and poles at  $E$  under the evaluation map  $\text{ev}_{\mathcal{P}}$ . If  $m < n$ , then the dimension of the code  $C_L(\mathcal{X}, \mathcal{P}, E)$  is at least  $m + 1 - g$  and its minimum distance is at least  $n - m$ . If  $m > 2g - 2$ , then its dimension is  $m + 1 - g$ . The dual code  $C_L(\mathcal{X}, \mathcal{P}, E)^\perp$  is again AG. If  $m > 2g - 2$ , then the dimension of the code  $C_L(\mathcal{X}, \mathcal{P}, E)^\perp$  is at least  $n - m - 1 + g$  and its minimum distance is at least  $d^* = m - 2g + 2$ , which is called the *designed minimum distance*. If  $m < n$ , then its dimension is  $n - m - 1 + g$ .

Algebraic geometry codes were proposed by Niederreiter [23] and Janwa-Moreno [12] for code-based PKC systems. This system was broken for genus zero [29], one and two [7, 22] and for arbitrary genus for so called VSAP codes [16, 17, 18, 19].

Let  $r = l(E) - 1$  and  $\{f_0, \dots, f_r\}$  be a basis of  $L(E)$ . Consider the following map:

$$\varphi_E : \mathcal{X} \longrightarrow \mathbb{P}^r(\mathbb{F}_q)$$

defined by  $\varphi_E(P) = (f_0(P) : \dots : f_r(P))$ . If  $m > 2g$ , then  $r = m - g$ . So  $\varphi_E$  defines an embedding of the curve  $\mathcal{X}$  of degree  $m$  in  $\mathbb{P}^r$ . More precisely, let  $\mathcal{Y} = \varphi_E(\mathcal{X})$ ,  $Q_j = \varphi_E(P_j)$  and  $\mathcal{Q} = (Q_1, \dots, Q_n)$ . Then  $\mathcal{Y}$  is a curve in  $\mathbb{P}^{m-g}$  of degree  $m$  and  $\varphi_E$  is an isomorphism from  $\mathcal{X}$  to  $\mathcal{Y}$ . Now  $\varphi_E(E) \equiv \mathcal{Y} \cdot H$  for every hyperplane  $H$  of  $\mathbb{P}^{m-g}(\mathbb{F}_q)$ . If moreover  $E$  is effective, then  $\varphi_E(E) = \mathcal{Y} \cdot H$  for some hyperplane  $H$  of  $\mathbb{P}^{m-g}(\mathbb{F}_q)$ . Let  $F = \varphi_E(E)$ , then  $(\mathcal{Y}, \mathcal{Q}, F)$  is a representation of  $\mathcal{C}$  that is strict isomorphic with  $(\mathcal{X}, \mathcal{P}, E)$ .

If  $m \geq 2g + 2$ , then  $I(\mathcal{Y})$  is generated by  $I_2(\mathcal{Y})$ . If moreover  $n > 2m$ , then  $I_2(\mathcal{Q}) = I_2(\mathcal{Y})$ . Now  $C_L(\mathcal{X}, \mathcal{P}, E)$  is called a *very strong algebraic geometry* (VSAG) code if

$$2g + 2 \leq m < \frac{1}{2}n \quad \text{or} \quad \frac{1}{2}n + 2g - 2 < m \leq n - 4.$$

It was shown that the representation by the triple  $(\mathcal{X}, \mathcal{P}, E)$  of a VSAG code  $C_L(\mathcal{X}, \mathcal{P}, E)$  is unique up to isomorphisms [16, 17, 18] and that such a triple can be retrieved efficiently [19].

## 4 Error-correcting pairs and arrays from VSAG codes

Let  $C = C_L(\mathcal{X}, \mathcal{P}, E)^\perp$  be an AG code on a curve of genus  $g$  with designed minimum distance  $d^*$  and  $m = \deg(E) > 2g - 2$ . Let  $A = C_L(\mathcal{X}, \mathcal{P}, E - F)$ ,  $B = C_L(\mathcal{X}, \mathcal{P}, F)$  and  $C = C_L(\mathcal{X}, \mathcal{P}, E)^\perp$ . Then  $\langle A * B \rangle \subseteq C^\perp$ . If moreover  $t = \lfloor (d^* - 1 - g)/2 \rfloor$  and  $\deg(F) = m - t - g$ , then  $(A, B)$  is a  $t$ -ECP over  $\mathbb{F}_q$  by [25, Theorem 1] and [26, Theorem 3.3]. So there are abundant ways to construct error-correcting pairs of an AG code.

This approach needs the efficient computation of the Riemann-Roch spaces  $L(F)$  and  $L(E - F)$  and such algorithms are available. If  $e$  is sufficiently large and  $m > 4g - 3$ , then there exists a  $\lfloor (d^* - 1)/2 \rfloor$ -ECP over  $\mathbb{F}_{q^e}$  by [28, Proposition 4.2], but no efficient way to obtain the pair is known.

In the following we construct ECP's directly using subspaces of  $\mathbb{F}_q^n$  and circumventing the use of the Riemann-Roch spaces. If we take  $F = (m - t - g)P_1$  where  $P_1$  is the first rational point of  $\mathcal{P}$ , then  $L(E - F)$  is a subspace of  $L(E)$ , and  $A = C_L(\mathcal{X}, \mathcal{P}, E - F)$  is a subspace of  $C^\perp = C_L(\mathcal{X}, \mathcal{P}, E)$ .

In fact  $A$  is the space of those codewords in  $C^\perp$  that are zero at the first position of multiplicity  $m - t - g$  and this multiplicity can be controlled, since we have computed  $I_2(\mathcal{Q})$  efficiently. Define  $B_0 = \langle A * C \rangle^\perp$ , then  $B_0^\perp = \langle A * C \rangle \subseteq B^\perp$ . So  $d(B_0^\perp) \geq d(B^\perp) > t$ . Hence  $(A, B_0)$  is a  $t$ -ECP for  $C$ . There is one technical detail, note that  $P_1$  is in the support of  $E - F$  and  $F$ , but there is a generalized way to define algebraic geometry codes, using a local parameter as explained in [19], where it is no longer necessary to assume that  $\mathcal{P}$  is disjoint from the support of the divisor  $E$  in the definition of the code  $C_L(\mathcal{X}, \mathcal{P}, E)$ .

Similarly we can decode up to  $\lfloor (d^* - 1)/2 \rfloor$  errors using arrays or well-behaving sequences and majority voting [4, 5, 9, 10, 11].

## References

- [1] A. Barg. Complexity issues in coding theory. In V.S. Pless and W.C. Huffman, editors, *Handbook of coding theory*, volume 1, pages 649–754. North-Holland, Amsterdam, 1998.
- [2] A. Becker, A. Joux, A. May, and A. Meurer. Decoding random binary linear codes in  $2^{n/20}$ : How  $1 + 1 = 0$  improves information set decoding. In *Advances in cryptology—EUROCRYPT 2012*, volume 7237 of *Lecture Notes in Comput. Sci.*, pages 520–536. Springer, Heidelberg, 2012.
- [3] E.R. Berlekamp, R.J. McEliece, and H.C.A. van Tilborg. On the inherent intractability of certain coding problems. *IEEE Transactions on Information*, 24:384–386, 1978.
- [4] I.M. Duursma. *Decoding codes from curves and cyclic codes*. PhD thesis, Eindhoven University of Technology, 1993.
- [5] I.M. Duursma. Majority coset decoding. *IEEE Transactions on Information Theory*, 39(3):1067–1070, 1993.
- [6] I.M. Duursma and R. Kötter. Error-locating pairs for cyclic codes. *IEEE Trans. Inform. Theory*, 40:1108–1121, 1994.
- [7] C. Faure and L. Minder. Cryptanalysis of the McEliece cryptosystem over hyperelliptic codes. In *Proceedings 11th Int. Workshop on Algebraic and Combinatorial Coding Theory, ACCT 2008*, pages 99–107, 2008.
- [8] G.L. Feng and T.R.N. Rao. Decoding algebraic-geometric codes up to the designed minimum distance. *IEEE Transactions on Information Theory*, 39(1):37–45, 1993.
- [9] G.L. Feng and T.R.N. Rao. A simple approach for construction of algebraic-geometric codes from affine plane curves. *IEEE Transactions on Information Theory*, 40(4):1003–1012, 1994.
- [10] G.L. Feng and T.R.N. Rao. Improved geometric goppa codes. I. basic theory. *IEEE Transactions on Information Theory*, 41(6):1678–1693, 1995.
- [11] O. Geil, R. Matsumoto, and D. Ruano. Feng-Rao decoding of primary codes. *Finite Fields and their Applications*, 23:35–52, 2013.
- [12] H. Janwa and O. Moreno. McEliece public crypto system using algebraic-geometric codes. *Designs, Codes and Cryptography*, 8:293–307, 1996.

- [13] C. Kirfel and R. Pellikaan. The minimum distance of codes in an array coming from telescopic semigroups. *IEEE Trans. Inform. Theory*, 41(6, part 1):1720–1732, 1995. Special issue on algebraic geometry codes.
- [14] R. Kötter. A unified description of an error locating procedure for linear codes. In *Proceedings of Algebraic and Combinatorial Coding Theory*, pages 113–117. Voneshta Voda, 1992.
- [15] R. Kötter. *On algebraic decoding of algebraic-geometric and cyclic codes*. PhD thesis, Linköping University of Technology, Linköping Studies in Science and Technology, Dissertation no. 419, 1996.
- [16] I. Márquez-Corbella, E. Martínez-Moro, and R. Pellikaan. Cryptanalysis of public-key cryptosystems based on algebraic geometry codes. *Oberwolfach Preprints*, OWP 2012-01:1–17, 2012.
- [17] I. Márquez-Corbella, E. Martínez-Moro, and R. Pellikaan. On the unique representation of very strong algebraic geometry codes. *Designs, Codes and Cryptography*, pages 1–16, 2013.
- [18] I. Márquez-Corbella, E. Martínez-Moro, and R. Pellikaan. Evaluation of public-key cryptosystems based on algebraic geometry codes. In *Proceedings of the Third International Castle Meeting on Coding Theory and Applications*, pages 199–204, Cardona Castle, Barcelona, September 11–15, 2011.
- [19] I. Márquez-Corbella, E. Martínez-Moro, R. Pellikaan, and D. Ruano. Computational aspects of retrieving a representation of an algebraic geometry code. *submitted to Designs, Codes and Cryptography*, 2013.
- [20] I. Márquez-Corbella and R. Pellikaan. A characterization of MDS codes that have an error-correcting pair. Lyngby, Denmark, 2012.
- [21] R.J. McEliece. A public-key cryptosystem based on algebraic coding theory. *DSN Progress Report*, 42–44:114–116, 1978.
- [22] L. Minder. *Cryptography based on error correcting codes*. PhD thesis, 3846 EPFL, 2007.
- [23] H. Niederreiter. Knapsack-type crypto systems and algebraic coding theory. *Problems of Control and Information Theory*, 15(2):159–166, 1986.
- [24] R. Pellikaan. On decoding linear codes by error correcting pairs. Preprint Technical University Eindhoven, 1988.
- [25] R. Pellikaan. On a decoding algorithm of codes on maximal curves. *IEEE Trans. Inform. Theory*, 35:1228–1232, 1989.
- [26] R. Pellikaan. On decoding by error location and dependent sets of error positions. *Discrete Math.*, 106–107:369–381, 1992.
- [27] R. Pellikaan. On the efficient decoding of algebraic-geometric codes. In *Eurocode '92 (Udine, 1992)*, volume 339 of *CISM Courses and Lectures*, pages 231–253. Springer, Vienna, 1993.
- [28] R. Pellikaan. On the existence of error-correcting pairs. *Statistical Planning and Inference*, 51:229–242, 1996.
- [29] V.M. Sidelnikov and S.O. Shestakov. On the insecurity of cryptosystems based on generalized Reed-Solomon codes. *Discrete Math. Appl.*, 2:439–444, 1992.

# Additive multivariable codes over $\mathbb{F}_4$

E. Martínez-Moro, A. Piñera-Nicolás  
Institute of Mathematics and Applied Math Department  
University of Valladolid, Spain  
{edgar, anicolas}@maf.uva.es

I. F. Rua  
Department of Mathematics  
University of Oviedo, Spain

## Abstract

The structure of additive multivariable codes over  $\mathbb{F}_4$  (the Galois field with 4 elements) is presented. This completes the study of the semisimple case that was specifically addressed by the same authors before. These codes extend in a natural way the abelian codes, of which additive are a particular case.

## Keywords

Additive Multivariable Codes, Abelian Codes, Quantum Codes

Quantum codes are designed to detect and correct the errors produced in quantum computations [6, 7]. These codes can be constructed with the help of specific classical codes, called *additive*, over  $\mathbb{F}_4$  (the Galois field with 4 elements) [1]. An additive code of length  $n$  is a subgroup of  $\mathbb{F}_4^n$  under addition. The particular case of additive cyclic codes has been considered in [2]. An additive code  $\mathcal{C}$  is called *cyclic* if, whenever  $c = (c_1 \dots c_n) \in \mathcal{C}$ , then its cyclic shift  $(c_2 \dots c_n c_1)$  is also a codeword in  $\mathcal{C}$ . These codes are related to properties of the ring  $\mathbb{F}_4[X]/\langle X^n - 1 \rangle$ . In the case  $n$  odd, the semisimple structure of this ring can be used to obtain a complete description of the codes [3]. The case  $n$  even has been also considered [4].

In this paper we describe additive multivariable codes over the finite field  $\mathbb{F}_4$  viewed as ideals of the quotient ring  $\mathbb{F}_4[X_1, \dots, X_r]/\langle t_1(X_1), \dots, t_r(X_r) \rangle$  (where  $t_i(X_i)X_i^{n_i} - 1 \in \mathbb{F}_4[X_i]$  are fixed polynomials). In the semisimple case (no-repeated roots) this structure was studied in [5]. The structure of the rings  $\mathcal{A}_4 = \mathbb{F}_4[X_1, \dots, X_r]/\langle t_1(X_1), \dots, t_r(X_r) \rangle$  and  $\mathcal{A}_2 = \mathbb{F}_2[X_1, \dots, X_r]/\langle t_1(X_1), \dots, t_r(X_r) \rangle$  is fundamental in this description.

## References

- [1] A. Calderbank, E. Rains, P. Shor, and N. Sloane. Quantum error correction via codes over  $\text{GF}(4)$ . *IEEE Trans. Inform. Theory*, 44:1369–1387, 1998.
- [2] B. Dey and B. Rajan.  $\mathbb{F}_q$ -linear cyclic codes over  $\mathbb{F}_q^m$ . *Des. Codes Cryptogr.*, 34:89–116, 2005.
- [3] W. C. Huffman. Additive cyclic codes over  $\mathbb{F}_4$ . *Adv. Math. Commun.*, 1(4):427–459, 2007.
- [4] W. C. Huffman. Additive cyclic codes over  $\mathbb{F}_4$ . *Adv. Math. Commun.*, 2(3):309–343, 2008.
- [5] E. Martínez-Moro, A.P. Nicolás and I. F. Rúa. Additive semisimple multivariable codes over  $\mathbb{F}_4$ . *Des. Codes Cryptogr.*, Accepted (Published Online) 45:1–20, 2012.
- [6] P. Shor. Scheme for reducing decoherence in quantum memory. *Phys. Rev. A*, 52, 1995.
- [7] A. Steane. Simple quantum error correcting codes. *Phys. Rev. Lett.*, 77:793–797, 1996.

# On Generalized Lee Weight Codes over Dihedral Groups

Edgar Martínez-Moro      Alejandro Piñera-Nicolás  
Emilio Suárez-Canedo

Institute of Mathematics and Applied Math Department  
University of Valladolid, Spain  
{edgar, anicolas, esuarez}@maf.uva.es

## Abstract

In this contribution we show the structure on some codes over non-Abelian groups, namely over  $D_{2^m}$  the dihedral group of  $2^m$  elements. We use the polycyclic presentation of  $D_{2^m}$  to give a natural extension of Lee metric in this case and propose a structure theorem for such codes.

## Keywords

Codes over Groups, Polycyclic Codes, Dihedral Groups

Group codes are a generalization of linear codes which its underlying structure is defined over an alphabet given by a group. These codes were first studied by Slepian in [7]. It has been shown in [3] that Abelian group codes for the Hamming metric do not achieve the capacity of arbitrary channels. It has also been conjectured that non-Abelian group codes are inferior to Abelian group codes [1, 4, 3] in that case. Recently in [6] they proved that there exist asymptotically good codes over non-abelian groups.

Whereas properties of group codes for Hamming metric have been extensively studied not too much is known in the non-abelian case for the Lee metric. Note that the Lee metric in the cyclic-group case has provided some nice and optimal non-linear binary codes as their Gray maps (see for example the seminal papers on this topic for block codes over  $\mathbb{Z}_4$  the cyclic group with 4 elements [5, 2]).

The first step when dealing with non-abelian groups is to consider the class of polycyclic groups. In this work we will consider codes over dihedral groups of  $2^{m+1}$  elements. Based on the polycyclic representation  $\text{pcp}(D_{2^m})$  of  $D_{2^m}$  we shall define the natural Lee metric on such codes that generalizes the well known Lee metric in the cyclic case. Based on the structure of  $\text{pcp}(D_{2^m})$  we shall derive a canonical form of this type of codes based on a chosen set of generators.

## References

- [1] G. David Forney On the Hamming distance properties of group codes. *IEEE Transactions on Information Theory* 38(6): 1797-1801 (1992).
- [2] A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé. The  $\mathbb{Z}_4$  linearity of Kerdock Preparata Goethals and related codes. *IEEE Trans. of Information Theory*, 40, (1994) 301–319.
- [3] C. Interlando, R. Palazzo, Jr. and M. Elia Group block codes over non-abelian groups are asymptotically bad. *IEEE Transactions on Information Theory*, vol. 42, No. 4, pp. 1277–1280, July 1996.
- [4] P. Massey. Many Non-Abelian Groups Support Only Group Codes That Are Conformant To Abelian Group Codes. *ISIT, 1997*. Ulm. Germany.
- [5] Alexandr A. Nechaev. Kerdock code in a cyclic form. *Diskr. Math. (USSR)*, 1 (1989), no. 4, 123–139 (in Russian). English translation *Discrete Math. Appl.*, 1, no. 4, 365–384 (1991).
- [6] Aria Ghasemian Sahebi and S. Sandeep Pradhan. Asymptotically Good Codes Over Non-Abelian Groups. <http://arxiv.org/abs/1202.0863>, 2012.
- [7] D. Slepian Group codes for the Gaussian Channel. *Bell. Syst. Tech. Journal*, 1962.

# Decoding of codes for applications to steganography

Carlos Munuera,  
University of Valladolid (Spain)

Wilson Olaya León  
Universidad Industrial de Santander (Colombia)

`cmunuera@arq.uva.es`

## Abstract

Error-correcting codes are introduced and widely for correcting errors when information is transmitted through noisy channels. A  $[n, k]$  linear error-correcting code is a  $k$ -dimensional linear subspace  $\mathcal{C} \subseteq \mathbb{F}_2^n$ . Errors are corrected by using a decoding map. This is a mapping  $\text{dec} : \mathcal{X} \rightarrow \mathcal{C}$ , where  $\mathcal{C} \subset \mathcal{X} \subseteq \mathbb{F}_2^n$  and  $\text{dec}(\mathbf{c}) = \mathbf{c}$  for all codeword  $\mathbf{c} \in \mathcal{C}$ .

Different criteria have been proposed for constructing decoding maps. The most common so far is *minimum distance*. Under this condition,  $\text{dec}(\mathbf{x})$  is taken as one of the nearest codewords to  $\mathbf{x}$ , with respect to the Hamming metric. It is well known that minimum distance decoding guarantees that we can recover the right information when the number of errors is not too big. The decoding  $\text{dec}$  is *complete* if  $\mathcal{X} = \mathbb{F}_2^n$ . Very few complete decoding methods are known, and except rare exceptions all of them are exponential in time and/or memory complexities. However completeness is not really a major problem in coding theory. Since the main goal is to recover the word sent by the sender, in most cases it is useless to obtain a different word as a result of our decoding, even being this word closest to the received vector. This is just the case when the nearest codeword is not unique. For this reason most efforts of coding-theorist have turned to find efficient bounded minimum distance decoding methods.

In recent times, new applications of coding theory have been found. In this presentation we are interested in steganography. Roughly speaking, the purpose of a steganographic system is to hide as much secret information as possible in a innocuous-like cover object (like a digital image), making as few changes as possible in the cover, to reduce the chance of being detected by third parties. This is done by using error-correcting codes and decoding maps.

In this new scenario, the classical choice of coding theorists –to dispense with the condition of complete decoding– is no longer valid. Indeed, if cannot decode then we cannot embed information, and our stegosystem does not work. Remark also that for error-correction purposes, errors of low weight are more probable, while for steganographic purposes, all vectors in  $\mathbb{F}_2^n$  are equally probable as covers.

Therefore, it seems appropriate now to consider new decoding algorithms, by relaxing the condition of minimum distance. In this talk we present the first steps in this study.

Let  $\mathcal{C}$  be a linear  $[n, k]$  code with distance  $d$  and systematic parity-check matrix  $\mathbf{H} = (\mathbf{H}' | \mathbf{I}_{n-k})$ . Let  $\mathbf{h}_1, \dots, \mathbf{h}_n$  be the columns of  $\mathbf{H}$  and let  $\mathbf{e}_1, \dots, \mathbf{e}_n$  be the canonical basis of  $\mathbb{F}_2^n$ . The syndrome of  $\mathbf{x} \in \mathbb{F}_2^n$  can be used to give an estimate of  $d(\mathbf{x}, \mathcal{C})$ . This leads to the following algorithm. Given a vector  $\mathbf{x} \in \mathbb{F}_2^n$ ,

- Input:** The vector  $\mathbf{x}$  to be decoded, the matrix  $\mathbf{H}$  in systematic form.
0. [Initialization]  $\mathbf{dec} \leftarrow \mathbf{x}$
  1. [Iteration] Repeat until  $\mathbf{s}(\mathbf{dec}) = \mathbf{0}$ :
    - find a coordinate  $i$  such that  $\text{wt}(\mathbf{s}(\mathbf{dec}) + \mathbf{h}_i)$  is minimum among all columns of  $\mathbf{H}$
    - set  $\mathbf{dec} \leftarrow \mathbf{dec} + \mathbf{e}_i$
    - recompute the syndrome  $\mathbf{s}(\mathbf{dec})$
  2. [Output]  $\mathbf{dec}$

requires at most  $\text{wt}(\mathbf{s}(\mathbf{x})) \leq n - k$  iterations and provides a decoding  $\text{dec}(\mathbf{x}) = \mathbf{dec}$  of  $\mathbf{x}$ .

Some properties of this decoding algorithm are the following.

- (a)  $d(\mathbf{x}, \text{dec}(\mathbf{x})) \leq \text{wt}(s(\mathbf{x}))$ .
- (b) is  $\text{wt}(s(\mathbf{x})) \leq d/2$  then  $\text{dec}(\mathbf{x})$  is the nearest codeword to  $\mathbf{x}$  in  $\mathcal{C}$ .
- (c)  $\rho(\text{dec}) \leq n - k$ .
- (d)  $\tilde{\rho}(\text{dec}) \leq (n - k)/2$ .

### Keywords

Error-correcting code, decoding, steganography

## References

- [1] A. Barg, Complexity issues in coding theory, in Handbook of Coding Theory, vol. 1. Edited by V. Pless, W. Huffman, R. Brualdi. North-Holland, 1998.
- [2] C. Munuera, Steganography from a coding theory point of view, in Algebraic geometry modeling in information theory. Edited by E. Martinez-Moro. World Scientific, 2012.



# On LDPC codes corresponding to new families of regular expanding graphs of large girth

Monika Polak, Vasyl Ustimenko  
Institute of Mathematics,  
Maria Curie-Skłodowska University (Poland)

`monika.katarzyna.polak@gmail.com`

## Abstract

We are testing correcting properties of LDPC codes connected with the new families of regular graphs of bounded degree and increasing girth. They form a family of expanding graphs, some of them are in fact Ramanujan graphs. In the difference with previously known graphs of large girth graphs from new families are not edge transitive. We compare spectral gaps and key parameters of LDPC codes for new graphs with previously known results. Some codes have visible advantage in comparison with codes obtained by Guinand and Lodge corresponding to connected components of family  $D(n, q)$  [7].

## Keywords

LDPC codes, expanding graphs, large girth, spectral gap

## 1 Introduction

There are many different algorithms in everyday life where graphs are used. One of the most interesting features of the new graphs is their expansion property. This property seems to be significant in a lot of mathematical, computational and physical contexts. Another interesting property of our graphs is the property of being a family of graphs of increasing girth. Such graphs are used for example for constructions of error correcting codes. In this short paper we briefly observe recent results on explicit constructions of families of expanding graphs of increasing girth.

Basically, only two explicit constructions of families of connected graphs of large girth and superlinear size are known (Ramanujan-Cayley graphs [12], algebraic graphs  $CD(n, q)$ ) given by the nonlinear system of equations over finite field  $F_q$ . Lubotzky, Phillips and Sarnak [24] proved that Ramanujan - Cayley graphs  $X(p, q)$ , where  $p$  and  $q$  are primes, introduced by G. Margulis [11] satisfy the Ramanujan graphs definition.

In this paper we present a method to obtain a new families of graphs with specific properties required in practical applications. We describe properties of obtained new families  $A'(n, q)$ ,  $A''(n, q)$ ,  $D'(n, q)$  in comparison to previously known families such as  $A(n, q)$  and  $D(n, q)$  which has been known since 1995 [10]. However the main goal is to show how they can be used in practice for the creation of error correcting codes.

By the theorem of Alon and Boppana, large enough members of an infinite family of  $q$ -regular graphs with constant  $q$  satisfy the inequality  $\lambda \geq 2\sqrt{d-1} - o(1)$ , where  $\lambda$  is the second largest eigenvalue in absolute value. Ramanujan graphs are  $d$ -regular graphs for which the inequality  $\lambda \leq 2\sqrt{d-1}$  holds.

We say that a family of regular graphs of bounded degree  $q$  of increasing order  $n$  has an expansion constant  $c$ ,  $c > 0$  if for each subset  $A$  of the vertex set  $X$ ,  $|X| = n$  with  $|A| \leq n/2$  the inequality  $|\partial A| \geq c|A|$  holds. The expansion constant of the family of  $q$ -regular graphs can be estimated via upper limit  $q - \lambda_n$ ,  $n \rightarrow \infty$ , where  $\lambda_n$  is the second largest eigenvalue of family representative of order  $n$ . It is clear that a family of Ramanujan graphs of bounded degree  $q$  has the best expansion constant.

Gregory Margulis constructed the first family of expanders via studies of Cayley graphs of large girth. Family of graphs  $G_n$  is a family of graphs of increasing girth if  $g(G_n)$  goes to infinity with the growth of  $n$ . The family of graphs of large girth is an infinite family of simple regular graphs

$\Gamma_i$  of degree  $k_i$  and order  $v_i$  such that:  $g(\Gamma_i) \geq \gamma \log_{k_i} v_i$ , where  $c$  is independent of  $i$  constant (see [1], [2]).

## 2 Construction of the families

Let  $F_q$ , where  $q$  is prime power, be a finite field.  $CD(n, q)$  (connected components of  $D(n, q)$ ) and  $A(n, q)$  are connected, biregular, bipartite  $V = P \cup L$  families of graphs of increasing girth. Graphs  $D(n, q)$ ,  $n \geq 2$  of fixed degree  $q$  form a family of expanders with the second largest eigenvalue bounded from above by  $2\sqrt{q}$ . A family  $A(n, q)$  of increasing girth, superlinear size and degree  $q$  is given by the nonlinear system of equations. If  $q$  is fixed then the second largest eigenvalue of  $A(n, q)$  is also bounded by  $2\sqrt{q}$ . So, families  $A(n, q)$  and  $D(n, q)$  consist of "almost Ramanujan graphs".

Let  $P$  and  $L$  be two copies of Cartesian power  $F_q^n$ , where  $n \geq 2$  is a integer. Brackets and parenthesis will allow the reader to distinguish points and lines. If  $z \in F_q^n$ , then  $(z) \in P$  and  $[z] \in L$ . First, we introduce the bipartite graph  $D(q)$  with the following points and lines, which are infinite dimensional vectors over  $F_q$  written in the following way

$$(p) = (p_{0,1}, p_{1,1}, p_{1,2}, p_{2,1}, p_{2,2}, p'_{2,2}, p_{2,3}, \dots, p_{i,i}, p'_{i,i}, p_{i,i+1}, p_{i+1,1}, \dots),$$

$$[l] = [l_{1,0}, l_{1,1}, l_{1,2}, l_{2,1}, l_{2,2}, l'_{2,2}, l_{2,3}, \dots, l_{i,i}, l'_{i,i}, l_{i,i+1}, l_{i+1,1}, \dots].$$

The point  $(p)$  is incident with the line  $[l]$  ( $(p)I[l]$ ), if the following relations between their coordinates hold:

$$\begin{cases} l_{1,1} - p_{1,1} = l_{1,0}p_{1,0} \\ l_{1,2} - p_{1,2} = l_{1,1}p_{1,0} \\ l_{2,1} - p_{2,1} = l_{0,1}p_{1,1} \\ l_{i,i} - p_{i,i} = l_{0,1}p_{i-1,i} \\ l'_{i,i} - p'_{i,i} = l_{i,i-1}p_{1,0} \\ l_{i,i+1} - p_{i,i+1} = l_{i,i-1}p_{1,0} \\ l_{i+1,i} - p_{i+1,i} = l_{0,1}p'_{i,i} \end{cases} \quad (1)$$

where  $i \geq 2$ . The set of vertices of the graph  $D(q)$  of this infinite structure is  $V = P \cup L$  and the set of edges consisting of all pairs  $\{(p), [l]\}$  for which  $(p)I[l]$ .

For each positive integer  $n > 2$  we obtain a finite incidence structure  $(P_n, L_n, I_n)_D$  as follows. Firstly,  $P_n$  and  $L_n$  are obtained from  $P$  and  $L$ , respectively, by projecting each vector onto its  $n$  initial coordinates with respect to the natural order. The incidence  $I_n$  is then defined by imposing the first  $n - 1$  incidence equations and ignoring all others. The graph corresponding to the finite incidence structure  $(P_n, L_n, I_n)$  is denoted by  $D(n, q)$ .  $D(n, q)$  become disconnected for  $n \geq 6$ . Graphs  $D(n, q)$  are edge transitive. It means that their connected components are isomorphic. Connected component of  $D(n, q)$  is denoted by  $CD(n, q)$ . Firstly LDPC codes based on graphs  $CD(n, q)$  were described in [7]. They are still in practical use. Notice that all connected components of infinite graph  $D(q)$  are  $q$ -regular trees.

Let us consider an alternative way of presentation of  $q$ -regular tree via equations over finite field  $F_q$ . We consider an infinite graph  $A(q)$  with the points and lines :

$$(p) = (p_{0,1}, p_{1,1}, p_{1,2}, p_{2,2}, p_{2,3}, \dots, p_{i,i}, p_{i,i+1}, \dots),$$

$$[l] = [l_{1,0}, l_{1,1}, l_{1,2}, l_{2,2}, l_{2,3}, \dots, l_{i,i}, l_{i,i+1}, \dots].$$

$A(q)$  is a graph of infinite incidence structure  $(P, L, I)_A$  such that point  $(p)$  is incident with the line  $[l]$  ( $(p)I[l]$ ), if the following relations between their coordinates hold:

$$\begin{cases} l_{i,i} - p_{i,i} = l_{1,0}p_{i-1,i} \\ l_{i,i+1} - p_{i,i+1} = l_{i,i}p_{0,1} \end{cases} \quad (2)$$

Like in the case of  $D(q)$  for each positive integer  $n > 2$  we obtain a finite incidence structure  $(P_n, L_n, I_n)_A$  where  $P_n$  and  $L_n$  are obtained from  $P$  and  $L$ , respectively, by projecting each vector onto its  $n$  initial coordinates with respect to the natural order. The incidence  $I_n$  is then defined by imposing the first  $n - 1$  incidence equations and ignoring all others. The graph corresponding to the finite incidence structure  $(P_n, L_n, I_n)$  is denoted by  $A(n, q)$ . Graphs  $A(n, q)$  are not edge transitive. They are connected if  $q \geq 2$ . In fact,  $A(n, q)$  form a family of small world graphs. There is a conjecture that  $CD(n, q)$  is another family of small world graphs.

Described families of graphs can be use to obtain new families with different structures. It can be done by use of simple cubical operator on the vertex set of graph from one of the family, such operator allow us to define a new relations. Let  $(v) = (v_1, v_2, \dots, v_n)$  denote point,  $[v] = [v_1, v_2, \dots, v_n]$  denote line and  $N_t(v)$  be the operator of taking neighbor of vertex  $v$  where first coordinate is  $v_1 + t$ :  $N_t(v_1, v_2, v_3, \dots, v_n) \rightarrow [v_1 + t, *, *, \dots, *]$ ,  $N_t[v_1, v_2, v_3, \dots, v_n] \rightarrow (v_1 + t, *, *, \dots, *)$ . The remaining coordinates can be determined uniquely using original relations defining used graph. As it follows from the equations each vertex has exactly one neighbor of chosen color  $t$ . It is easy to see that  $N_t$  is invertible operator on the set of vertices. To create a new family we can use the composition of two such operators  $N_t \circ N_0$  on two copies of the same graph ( it is also possibility to take other composition of such operators). For arbitrary graph  $G$  described above let  $I'$  denote the incidence relation defined by using composition  $N_t \circ N_0$ . Take two copies of  $G$  and denote point in first copy by  $(p)$  and in second by  $\langle z \rangle$ .  $(p)I' \langle z \rangle$  if for some  $t \in F_q$  relations  $(p)I[l]I \langle z \rangle$  hold, where  $I$  is the incidence relation ((1) or (2)) in based graph  $A(n, q)$  or  $D(n, q)$  described above. Both families of graphs have a natural coloring of vertices  $\rho$ . We simply assume that the color  $t = \rho(v)$  of the vertex  $v$  (point  $(p)$  or line  $[l]$ ) is its first coordinate  $p_{0,1}$  or  $l_{1,0}$ .

Let us define new binary relation on two copies of graph  $A(n, q)$ :  $(p)I' \langle z \rangle \Leftrightarrow$  when there exist  $t \in F_q$  such that the following relations holds:

$$\begin{cases} p_{0,1} = z_{0,1} - t \\ p_{1,1} = z_{1,1} + tp_{1,0} \\ p_{1,2} = z_{1,2} + tp_{1,1} + tz_{0,1}p_{0,1} \\ p_{2,2} = z_{2,2} - tz_{0,1}p_{1,1} - tz_{0,1}^2p_{0,1} \\ p_{i,i+1} = z_{i,i+1} + tp_{i,i} + tz_{0,1}p_{i-1,i} \\ p_{i+1,i+1} = z_{i+1,i+1} - tz_{0,1}p_{i,i} - tz_{0,1}^2p_{i-2,i-1} \end{cases} \quad (3)$$

for  $i \geq 2$ . Let denote a graph described by this system of equations by  $A'(n, q)$ .

Graphs  $D'(n, q)$  with the notation for point and line as for  $D(n, q)$  is described by the following relations (for  $t \in F_q$ ):

$$\begin{cases} p_{0,1} = z_{1,0} - t \\ p_{1,1} = z_{1,1} + tz_{0,1} \\ p_{1,2} = z_{1,2} + tp_{1,1} + tz_{0,1}p_{0,1} \\ p_{2,1} = z_{2,1} - tz_{1,0}z_{1,0} \\ p_{i,i} = z_{i,i} - tz_{0,1}p_{i-1,i-1} - tp_{0,1}z_{0,1}^2 \\ p'_{i,i} = z'_{i,i} + tp_{i,i-1} + tz_{0,1}p_{i-1,i-1} \\ p_{i,i+1} = z_{i,i+1} + tp_{i,i} + tz_{0,1}p_{i-1,i} \\ p_{i+1,i} = z_{i+1,i} - tz_{0,1}p_{i,i-1} - tz_{0,1}^2p_{i-1,i-1} \end{cases} \quad (4)$$

for  $i \geq 2$ . All above mentioned constructions form a simple undirected families of graphs. Expansion and other properties are shown below.

**Proposition 1**

Families  $A'(n, q)$  and  $D'(n, q)$  are expanders.

**Proposition 2**

Families  $A'(n, q)$  and  $D'(n, q)$  for  $q = 3$  are  $q$ -regular Ramanujan graphs  $\lambda_1 \leq 2\sqrt{3-1}$  and they density is  $\frac{4}{3(3^{n+1}-1)}$ .

**Proposition 3**

Families  $A'(n, q)$  and  $D'(n, q)$  are families of graphs of increasing girth (with growing  $n$ ). For all  $n \geq 2$  there is no cycles of length 4.  $D'(n, q)$  form a family of a large girth.

**Proposition 4**

There is no transitive groups defined on the graphs  $A'(n, q)$  and  $D'(n, q)$ .

### 3 Corresponding LDPC codes

Presented construction leads us to families of graphs that can be successfully used in coding theory to create LDPC codes.

Margulis and other authors for gave an interesting construction of error correcting codes LDPC based on expanders from the family of Cayley - Ramanujan , but in 2003 D. MacKay together with M. Postol showed the weaknesses of this construction [21]. These codes include the codewords of small weight, thus they can't be used in practice. Since 1997 when the first time graphs  $CD(n, q)$  have been used to create LDPC codes, which are applied by NASA there were no results, that

would indicate a weak properties of codes derived from them. Therefore very good and economic codes can be obtained by studying algebraic structures with similar properties.

To create LDPC code with codeword of length  $N$  we use  $A'(n, q)$  or  $D'(n, q)$  where  $n^q > N$ . Each of these graphs is already bipartite but  $q$ -regular instead of biregular. We can make it by the method described for graphs  $D(n, q)$  in [10]. Bidegree reduction can only increase the girth so there is no short cycles. After bidegree reduction the graph can be disconnected and divided into several components. To create a parity checks matrix we use to only one component. We decide to put one or zero in a parity check matrix by checking if relations (3) or (4) on coordinates of individual points and lines are satisfied. Reducing bidegrees to  $e < q$  and  $f$  gives code rate  $1 - \frac{e}{f}$ .

It can be proved that these new families of graphs have increasing girth (with increasing  $n$ ) and are not edge transitive, so we can call them pseudorandom. This is the reason why obtained codes have different properties for different chosen parameters (subset  $A$  and  $B$  described below). In a case of graphs  $A(n, q)$  and  $D(n, q)$  it does not matter which elements contain the subsets  $A$  and  $B$ , we are only interested in how many elements they contain. Graphs from these families do not have short cycles ( length 4 or less) so this fact provides the convergence of decoding algorithm.

Let consider the minimum distance analysis for described codes. Presented families of graphs have increasing girth so we can construct LDPC codes with arbitrary large girth. In [17] Tanner proved the following lower bound on  $d_{min}$  in terms of girth  $g$  and bit node degree  $e$ :

$$d_{min} \geq \frac{2[(e-1)^{g/4} - 1]}{e-2}, \text{ where } g/2 \text{ is even}$$

$$d_{min} \geq \frac{[e(e-1)^{\lfloor g/4 \rfloor} - 2]}{e-2}, \text{ where } g/2 \text{ is odd}$$

Combining Proposition 3 and above mentioned inequalities, we see that LDPC codes, corresponding to presented families of graphs, can be designed to have arbitrarily large minimum distance  $d_{min}$ .

We were testing LDPC codes corresponding to designed families of graphs by using BPSK modulation over AWGN channel and simple MAP decoder implementation. Our simulations showed that codes, based on representatives of new described families, have most frequently better error correcting properties than codes based on  $D(n, q)$ . This fact is supported by many simulations conducted for randomly chosen parameters. Fig. 1 shows the relationship between bit error rate (the ratio of number of received incorrect bits to total length of received codeword) and power of signal.

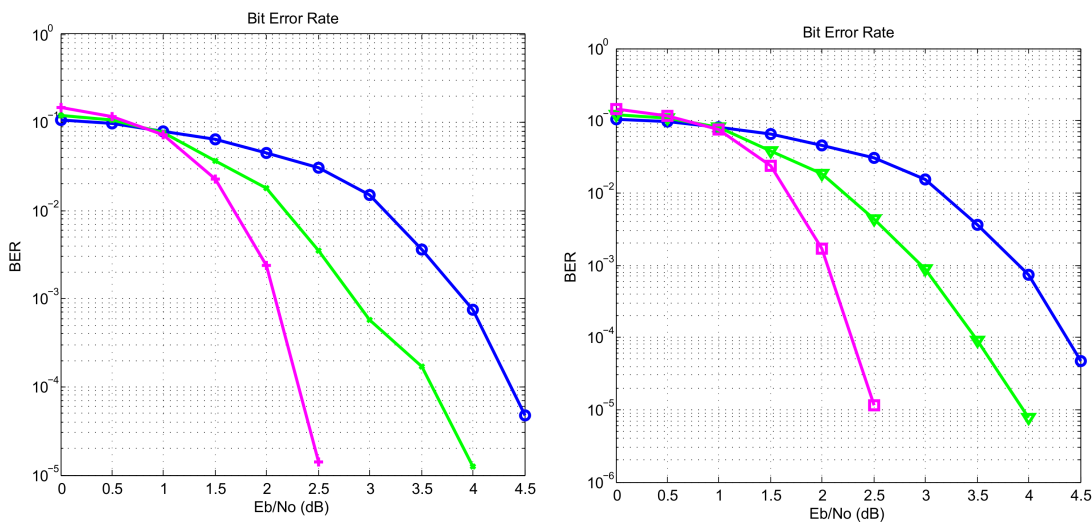


Figure 1: Bit error rate for codes based on graphs  $D'(n, q)$  on left side and based on graphs  $A'(n, q)$  on right side, with parameters:  $n = 6$  and  $q = 7$ —blue,  $n = 3$  and  $q = 7$ —green,  $n = 5$  and  $q = 5$ —purple.

## References

- [1] N. Biggs, Algebraic Graph Theory (2nd ed), Cambridge, University Press, 1993.
- [2] N.L. Biggs, Graphs with large girth , *Ars Combinatoria*, 25C (1988), 7380.
- [3] B. Bollobas, Extremal Graph Theory. Academic Press, 1978.
- [4] A. Brower, A. Cohen, A. Nuemaier, Distance regular graphs, Springer, Berlin, 1989.
- [5] R. G. Gallager, Low-Density Parity-Checks Codes, *IRE Trans of Info Thy* 8 (Jan 1962):21–28.
- [6] P. Guinand, J. Lodge, Graph theoretic construction of generalized product codes, *IEEE International Symposium on Information Theory ISIT'97 Ulm, Germany* (June 29-July 4 1997):111.
- [7] P. Guinand, J. Lodge, Tanner type codes arising from large girth graphs, *Canadian Workshop on Information Theory CWIT '97, Toronto, Ontario, Canada* (June 3-6 1997):5–7.
- [8] W. C. Huffman, V. Pless, Fundamentals of error correcting codes, first edition, Cambridge University Press, Cambridge, 2003.
- [9] F. Lazebnik, V. A. Ustimenko, A. J. Woldar, A characterization of the components of the graphs  $D(k, q)$ , *Discrete Mathematics* Vol. 157 (1996):271–283.
- [10] F. Lazebnik, V. A. Ustimenko and A. J. Woldar, A new series of dense graphs of high girth , *Bulletin (New Series) of the AMS* Vol. 32, Number 1 (1995):73–79.
- [11] G. A. Margulis. Explicit group-theoretic constructions of combinatorial schemes and their applications in the construction of expanders and concentrators. *Problemy Peredachi Informatsii*, 24(1):5160, 1988
- [12] G. A. Margulis, Explicit construction of graphs without short cycles and low density codes, *Combinatorica*, 2, (1982), 71-78
- [13] C. E. Shannon, A Mathematical Theory of Communication, *Bell System Technical Journal* Vol. 27 (1948):379–423, 623–656.
- [14] C. E. Shannon, W. Warren, *The Mathematical Theory of Communication*, University Of Illinois Press, 1963.
- [15] T. Shaska, W. C. Huffman, D. Joener and V. Ustimenko (editors), *Advances in Coding Theory and Cryptography*, Series on Coding and Cryptology Vol. 3 (2007):181–200.
- [16] A. Shokrollahi, LDPC Codes: An Introduction, Digital Fountain Inc, Fremont (2002), available from: <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.110.1008>.
- [17] R. M. Tanner, A recursive approach to low density codes, *IEEE Transactions on Information Theory* IT 27(5) (1984):533–547.
- [18] R. Weiss, Distance transitive graphs and generalised polygons , *Arch. Math*, 45, 1985, pp.186-192.
- [19] Luby M. G., Mitzenmacher M., Shokrollahi M. A., Spielman D. A., Improved Low-Density Parity- Check Codes Using Irregular Graphs and Belief Propagation, in *ISIT 98-IEEE International Symposium of Information Theory, Cambridge, USA* (1998): 171.
- [20] MacKay D. J. C., Neal R. M., Good Codes Based on Very Sparse Matrices, in *Cryptography and Coding 5th IMACConference, BERLIN* (1995): 100.
- [21] D. MacKay and M. Postol, Weakness of Margulis and Ramanujan Margulis Low Density Parity Check Codes , *Electronic Notes in Theoretical Computer Science*, 74 (2003), 8pp.
- [22] Sipser M., Spielman D. A., Expander codes, *IEEE Trans on Info Theory* 42 (6) (1996): 1710.
- [23] Margulis G. A., Explicit construction of graphs without short cycles and low density codes, // *Combinatorica*.- 2.- 1982, - P. 71-78.
- [24] Lubotsky A., R. Philips R., P. Sarnak P. Ramanujan graphs// *J. Comb. Theory*.- 115,- N 2.-1989 .- P, 62-89.

# Representation, constructions and minimum distance computation of binary nonlinear codes

Jaume Pujol, Mercè Villanueva, and Fanxuan Zeng  
 Universitat Autònoma de Barcelona  
 fanxuan@deic.uab.cat

## Abstract

Let  $\mathbb{Z}_2$  be the ring of integers modulo 2 and let  $\mathbb{Z}_2^n$  be the set of all binary vectors of length  $n$ . The *Hamming distance*  $d(u, v)$  between two vectors  $u, v \in \mathbb{Z}_2^n$  is the number of coordinates in which  $u$  and  $v$  differ. The *Hamming weight*  $wt(u)$  of  $u \in \mathbb{Z}_2^n$  is  $wt(u) = d(u, \mathbf{0})$ , where  $\mathbf{0}$  is the all-zero vector of length  $n$ . A  $(n, M, d)$  *binary code*  $C$  is a subset of  $\mathbb{Z}_2^n$  with  $M$  codewords and minimum Hamming distance  $d$ . The *minimum Hamming distance*, denoted by  $d(C)$ , is the minimum value of  $d(u, v)$  for all  $u, v \in C$  and  $u \neq v$ .

Two binary codes  $C_1$  and  $C_2$  of length  $n$  are said to be *equivalent* if there exists a vector  $a \in \mathbb{Z}_2^n$  and a coordinate permutation  $\pi$  such that  $C_2 = \{a + \pi(c) : c \in C_1\}$ . Note that two equivalent codes have the same minimum distance. If  $C$  is linear, then  $\mathbf{0} \in C$ ; but if  $C$  is nonlinear, then  $\mathbf{0}$  does not need to belong to  $C$ . In this case, we can always consider a new binary code  $C' = C + c$  for any  $c \in C$ , which is equivalent to  $C$ , such that  $\mathbf{0} \in C'$ . Therefore, from now on, we assume that  $\mathbf{0} \in C$ .

Given a binary code  $C$ , the problem of storing  $C$  in memory is a well known problem. If  $C$  is linear, that is, it is a subgroup of  $\mathbb{Z}_2^n$ , then it can be compactly represented using a binary generator matrix. On the other hand, if  $C$  is nonlinear, then a solution would be to know whether it has another structure or not. For example, there are binary codes which have a  $\mathbb{Z}_4$ -linear or  $\mathbb{Z}_2\mathbb{Z}_4$ -linear structure and, therefore, they can also be compactly represented using a quaternary generator matrix. In general, binary codes without any of these structures can be represented as the union of cosets of a binary linear subcode of  $C$ . This allows us to represent them as a set of representative codewords instead of as a set with all codewords.

The *kernel* of a binary code  $C$  is defined as  $K(C) = \{x \in \mathbb{Z}_2^n : x + C = C\}$ . Since  $\mathbf{0} \in C$ ,  $K(C)$  is a binary linear subcode of  $C$ . We denote by  $k$  the dimension of  $K(C)$ . In general,  $C$  can be written as the union of cosets of  $K(C)$ , and  $K(C)$  is the largest such linear code for which this is true [1]. Therefore,

$$C = \bigcup_{i=0}^t \left( K(C) + c_i \right), \quad (1)$$

where  $c_0 = \mathbf{0}$ ,  $t + 1 = M/2^k$  and  $M = |C|$ . Note that we can represent  $C$  as the kernel  $K(C)$  plus the coset leaders  $L = \{c_1, \dots, c_t\}$ . It is important to emphasize that the codewords in  $L$  are not necessarily the ones having minimum weight in the coset. Since  $K(C)$  is linear, it can be compactly represented by its binary generator matrix  $G$  of size  $k \times n$ . Therefore, considering  $L$  as the matrix where in the  $t$  rows there are the coset leaders, the binary code  $C$  can be also represented by the matrix  $\begin{pmatrix} G \\ L \end{pmatrix}$ . Since the kernel takes up a memory space of order  $O(nk)$ , the kernel plus the  $t$  coset leaders take up a memory space of order  $O(n(k+t))$ .

For example, applying this representation to the set of all completely classified binary perfect codes of length 15 and extended perfect codes of length 16, we obtain very significant compression rates. It is known that there are exactly 5983 binary perfect codes of length 15 and 2165 binary extended perfect codes of length 16, each one having 2048 codewords [2]. In the first case, instead of taking up  $5983 \cdot 2048 \cdot 4 = 49012736$  hexadecimal numbers by encoding each codeword in hexadecimal notation, it only takes 3677928 hexadecimal numbers by storing the codewords of a generator matrix of the kernel and the set of coset leaders for each binary code. This gives a compression rate of 92.5%. Similarly, in the second case, the extended perfect codes of length 16 can be compressed from  $2165 \cdot 2048 \cdot 4 = 17735680$  hexadecimal numbers to 1439336, which gives a compression rate of 91.9%.

In order to compute the kernel and coset leaders of a binary code  $C$  of length  $n$ , according to the definition of  $K(C)$ , it is necessary to classify the  $M$  codewords of  $C$ . Since  $M = 2^k(t+1)$ , the algorithm must be at least exponential on  $k$ , the dimension of  $K(C)$ . A straightforward algorithm to compute the kernel from the definition of  $K(C)$  requires  $M^2 \log M$  operations,

if  $C$  is sorted. However, this algorithm can be improved using the following two properties: (1) if  $K' \subseteq K(C)$ , then  $v \in K(C)$  if and only if  $K' + v \subseteq K(C)$ ; (2) if  $K' \subseteq K(C)$ ,  $v \in C$  and  $(C \setminus K') + v \subseteq C$ , then  $v \in K(C)$ . Therefore, depending on  $k$ , the complexity can be reduced. If  $k = 0$  we still need  $M^2 \log M$  operations, but if  $k > 0$  we obtain a complexity of order  $O(kM \log M)$ . Note that, for large  $M$ ,  $kM \ll M^2$ .

Although the exponential behaviour of the kernel computation, using the representation given above, we can manipulate and construct new binary nonlinear codes from old ones in a more efficient way. Specifically, we show how to establish the equality and inclusion of two given nonlinear codes from their kernels and coset leaders, and how to compute the kernel and coset leaders of related new codes (union, intersection, extended, punctured, shorten, direct sum, Plotkin sum) from given ones, which are represented in this structure. All these results will be written to be implemented easily as algorithms.

Given a binary code  $C$ , the problem of computing its minimum distance is also important, and necessary in order to establish its error-correcting capability. This problem is computationally difficult, and has been proven to be NP-hard. If  $C$  is linear, the minimum distance coincides with the minimum weight, denoted by  $wt(C)$ , and the Brouwer-Zimmerman minimum weight algorithm for linear codes over finite fields [3] can be used. We propose new algorithms to compute the minimum weight and minimum distance of a binary nonlinear code  $C$ , based on the coset structure and the known algorithms for linear codes. Given a binary code  $C$  and a vector  $v \in \mathbb{Z}_2^n$ , let  $K_v = K(C) \cup (K(C) + v)$ . Since  $K(C)$  is linear, then  $K_v$  is also linear.

**Proposition 1** *Let  $C = \bigcup_{i=0}^t (K(C) + c_i)$  with  $t \geq 2$ . Then, the minimum weight of  $C$  can be computed as  $\min(\{wt(K_{c_i}) : i = 1, \dots, t\})$ , and the minimum distance as  $\min(\{wt(K_{c_i}) : i = 1, \dots, t\} \cup \{wt(K_{c_i+c_j}) : i, j = 1, \dots, t \text{ and } i < j\})$ .*

Using Proposition 1 and applying the known Brouwer-Zimmermann algorithms, we can compute the minimum weight and distance of a binary nonlinear code. Note that the complexity of these two algorithms depends strongly on the number of coset leaders  $t$ . For the minimum weight, we compute  $t$  times the minimum weight of a linear code  $K_v$ , and for the minimum distance,  $\binom{t+1}{2}$  times. An estimate of the total work an algorithm performs is referred to as *work factor* [4]. We study the work factors for these algorithms to compare them with brute force. An improvement is given to the proposition by avoiding repeated computations in each coset.

Finally, the previous algorithm can also be used to decode a binary linear code  $C$ . For a received vector  $u \in \mathbb{Z}_2^n$ , in order to decode it as a codeword from  $C$ , we look for a vector  $e$  of minimum weight such that  $u - e \in C$ . This is equivalent to find a vector  $e$  of minimum weight in the coset containing  $u$ , which is  $C + u$ .

**Proposition 2** *Let  $C$  be a binary linear code with minimum distance  $d$ . For a received vector  $u = c + e \notin C$ , where  $c \in C$ , let  $C_u = C \cup (C + u)$ . If  $wt(e) < d$ , then the received vector  $u$  can be decoded as  $c' = u - e' \in C$ , where  $e'$  is a vector of minimum weight in  $C_u$ , so  $wt(e) = wt(e')$ . Note that if  $wt(e) \leq \lfloor \frac{d-1}{2} \rfloor$ , then  $e' = e$  and  $c' = c$ .*

In this way, we can decode a received vector as long as less than  $d$  errors have been added to the transmitted codeword. When  $d$  or more than  $d$  errors occurs during the transmission, the minimum vector of  $C_u$  could come from  $C$ , and an error vector  $e$  can not be found. Therefore, the method provides a complete decoding but only up to  $d - 1$  errors. Note that if the covering radius of  $C$ , denoted by  $\rho$ , satisfies  $\rho \leq d - 1$ , that is when  $C$  is a maximal code, we actually obtain a complete decoding.

### Keywords

binary nonlinear codes, kernel, minimum distance, decoding

## References

- [1] H. Bauer, B. Ganter and F. Hergert, "Algebraic techniques for nonlinear codes," *Combinatorica*, vol. 3, pp. 21-33, 1983.
- [2] P. R. J. Östergård and O. Pottonen, "The perfect binary one-error-correcting codes of length 15: part I-classification." *IEEE Trans. Inform. Theory*, vol. 55, no. 10, pp. 4657-4660, 2009.
- [3] K.-H. Zimmerman, "Integral Hecke Modules, Integral Generalized Reed-Muller Codes, and Linear Codes," Tech. Rep. 3-96, Technische Universität Hamburg-Harburg, 1996.
- [4] G. White, "Enumeration-based Algorithms in Coding Theory," PhD Thesis, University of Sydney, 2006.

# On regular forests given in terms of algebraic geometry, new families of expanding graphs with large girth and new multivariate cryptographical algorithms

Urszula Romańczuk, Vasyl Ustymenko  
Maria Curie-Skłodowska University in Lublin (Poland)

urszula\_romanczuk@yahoo.pl, vasy1@hektor.umcs.lublin.pl

## EXTENDED ABSTRACT

We are going to observe interpretations of  $q$ -regular forest ( $q$ -regular simple graph without cycles) in terms of algebraic geometry over finite field  $\mathbb{F}_q$ . More precisely we are interested in sequences of  $q$ -regular algebraic graphs  $\Gamma_i$ , defined by nonlinear equations, such that their projective limit  $T$  is well defined and does not contain cycles. So, the girth of  $\Gamma_i$  is growing with the growth of parameter  $i$ . We assume additionally that  $\Gamma_i$ ,  $i \rightarrow \infty$  is a family of expanders. So the upper limit of second largest eigenvalues of  $\Gamma_i$  is bounded away from  $q$ .

The talk is dedicated to new applications of such simple graphs of increasing girth with good expansion properties to the and designing of cryptographical algorithms (stream ciphers, key exchange protocols, public key algorithms digital signatures, constructions of hash functions). We speak about the usage of classical explicit constructions (see [6] and further references) as well as applications of the new families of graphs.

Recall that the girth is the length of minimal cycle in the simple graph. Studies of maximal size  $ex(C_3, C_4, \dots, C_{2m}, v)$  of the simple graph on  $v$  vertices without cycles of length  $3, 4, \dots, 2m$ , i.e. graphs of girth  $> 2m$ , form an important direction of Extremal Graph Theory. As it follows from famous Even Circuit Theorem by P. Erdős' we have inequality

$$ex(C_3, C_4, \dots, C_{2m}, v) \leq cv^{1+1/m},$$

where  $c$  is a certain constant. The bound is known to be sharp only for  $m = 2, 3, 5$ . The first general lower bounds of kind

$$ex(v, C_3, C_4, \dots, C_n) = \Omega(v^{1+c/n}),$$

where  $c$  is some constant  $< 1/2$  were obtained in the 50th by Erdős' via studies of *families of graphs of large girth*, i.e. infinite families of simple regular graphs  $\Gamma_i$  of degree  $k_i$  and order  $v_i$  such that

$$g(\Gamma_i) \geq c \log_{k_i} v_i,$$

where  $c$  is the independent of  $i$  constant. Erdős' proved the existence of such a family with arbitrary large but bounded degree  $k_i = k$  with  $c = 1/4$  by his famous probabilistic method.

Just two explicit families of regular simple graphs of large girth with unbounded girth and arbitrarily large  $k$  are known: the family  $X(p, q)$  of Cayley graphs for  $PSL_2(p)$ , where  $p$  and  $q$  are primes, had been defined by G. Margulis [5] and investigated by A. Lubotzky, Sarnak [2] and Phillips, and the family of algebraic graphs  $CD(n, q)$  [3]. The best known lower bound for  $d \neq 2, 3, 5$  had been deduced from the existence of mentioned above families of graphs

$$ex(v, C_3, C_4, \dots, C_{2d}) \geq c(v^{1+2/(3d-3+e)})$$

where  $e = 0$  if  $d$  is odd, and  $e = 1$  if  $d$  is even.

By the theorem of Alon and Boppana, large enough members of an infinite family of  $q$ -regular graphs satisfy the inequality  $\lambda \geq 2\sqrt{q-1} - o(1)$ , where  $\lambda$  is the second largest eigenvalue in absolute value. Ramanujan graphs are  $q$ -regular graphs for which the inequality  $\lambda \leq 2\sqrt{q-1}$



holds. We say that regular graphs of bounded degree  $q$  form a family of Ramanujan graphs if the second largest eigenvalue of each graph is bounded from above by  $2\sqrt{q-1}$

It is clear that a family of Ramanujan graphs of bounded degree  $q$  has the best possible spectral gap  $q - \lambda$ . We say, that family of  $q$ -regular graphs  $\Gamma_i$  is a family of *almost Ramanujan graphs* if its second largest eigenvalues are bounded above by  $2\sqrt{q}$ .

The mentioned above family  $X(p, q)$  is a family of Ramanujan graphs. That is why we refer to them as Cayley - Ramanujan graphs. The family  $CD(n, q)$  is a family of almost Ramanujan graphs. It is known that if  $q \geq 5$  these graphs are not Ramanujan despite the projective limit  $CD(q)$  of  $CD(n, q)$  is a  $q$ -regular tree. The reason is that the eigenspace of  $CD(q)$  is not a Hilbert space (topology is  $p$ -adic).

Expanding properties of  $X(p, q)$  and  $D(n, q)$  and the high girth property of both families can be used for the construction of fast stream ciphers with good mixing properties[8]. Notice that both properties had been use for construction of good class of LDPC error correcting codes which is an important practical tool of security for satellite communications. The usage of  $CD(n, q)$  as Tanner graphs producing LDPC codes lead to better properties of corresponding codes in the comparison with the use of Cayley - Ramanujan graphs (see [4]).

Both families  $X(p, q)$  and  $CD(n, q)$  are consist of edge transitive graphs, their expansion properties and property to be graphs of large girth hold also for random graphs, which have no automorphisms at all. To make better deterministic approximation of random graph we can look at regular expanding graphs of increasing girth without edge transitive automorphism group (see [7]).

**THEOREM** *For each prime power  $q, q \geq 3$  there exist a family of  $q$ -regular bipartite almost Ramanujan graphs of large girth without edge transitive automorphism group.*

The proof of the theorem is based on new explicit construction of the families satisfying condition of formulated above theorem. The new cryptographical algorithms based on walks of new graphs and their analogs defined over arithmetical rings will be presented at the conference.

The important direction of Multivariate Cryptography is a search for a families of invertible polynomial maps  $f_n$  of  $\mathbb{F}_q^n$  with the degree bounded degree (usually degrees are 2 or 3), such that the growth of degree  $f_n^{-1}$  with the growth of  $n$  is supported by mathematical statement (see [1] an further references). Absence of mathematical theory here motivates alternative research on cryptographical applications of computable multivariate functions  $f_n$  with the degree  $cn, c > 0$  for  $f_n$  and its inverse.

We present pseudocubical cryptosystem from this class, such that the list of cubical public rules are given in terms of standard variables  $x_1, x_2, \dots, x_n$  corresponding to characters from the plainspace and extra characters  $y_1, y_2, \dots, y_t$ , where  $t = f(n)$  is a certain linear function from  $n$ . The list of rules is of kind

$$x_i \rightarrow g_i(x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_t), \quad i = 1, 2, \dots, n,$$

where  $f_i$  are cubical expressions and recursive "compression rules":

$$\begin{aligned} y_1 &\rightarrow h_1(x_1, x_2, \dots, x_n), \\ y_2 &\rightarrow h_2(x_1, x_2, \dots, x_n, y_1), \\ y_3 &\rightarrow h_3(x_1, x_2, \dots, x_n, y_1, y_2), \\ &\dots \\ y_t &\rightarrow h_t(x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_{t-1}). \end{aligned}$$

The resulting encryption map has degree  $cn, c \geq 1/4$ . So the algorithm is resistant against plain linearisation attacks. We can prove that the order of the map is growing to infinity with the growth of parameter  $n$ .

Traditionally one subset of vertices of a bipartite graphs is denoted by  $V_1 = P$  and called a set of points and another one  $V_2 = L$  is called a set of lines. Let  $K$  be a commutative ring,  $P$  and  $L$  be two copies of Cartesian power  $K^n$ , where  $n \geq 2$  is an integer. Brackets and parenthesis will allow the reader to distinguish points and lines. In this note we assume that if  $z \in K^n$ , then  $(z) \in P$  and  $[z] \in L$ .

Let us introduce an infinite bipartite graph  $D(K)$  defined on sets of points of kind

$$(x) = (x_1, x_2, x_3, x'_3, \dots, x_n, x'_n, \dots)$$

and lines of kind

$$[y] = [y_1, y_2, y_3, y'_3, \dots, y_n, y'_n, \dots]$$

via incidence relation  $I : (x)I[y]$  if and only if the following relations hold

$$\begin{aligned} x_2 - y_2 &= y_1 x_1, \\ x_3 - y_3 &= x_1 y_2, \\ x_4 - y_4 &= y_1 x_3, \\ x_5 - y_5 &= x_1 y_4, \\ &\dots \end{aligned}$$

together with equalities

$$\begin{aligned} x'_3 - y'_3 &= y_1 x_2, \\ x'_4 - y'_4 &= x_1 y'_3, \\ x'_5 - y'_5 &= y_1 x'_4, \\ &\dots \end{aligned}$$

If  $n$  is odd then  $x_n - y_n = x_1 y_{n-1}$  and  $x'_n - y'_n = y_1 x'_{n-1}$ . If  $n$  is even then  $x_n - y_n = y_1 x_{n-1}$  and  $x'_n - y'_n = x_1 y'_{n-1}$ .

We also consider the family of graphs  $B(m, n, K)$  for case  $m \leq n$ , whose vertices are points of kind

$$(x) = (x_1, x_2, x_3, x'_3, \dots, x_{m+2}, x'_{m+2}, x'_{m+3}, x'_{m+4}, \dots, x'_{n+2})$$

from set  $P_{m,n} = K^{m+n+2}$  and lines of kind

$$[y] = [y_1, y_2, y_3, y'_3, \dots, y_{m+2}, y'_{m+2}, y'_{m+3}, y'_{m+4}, \dots, y'_{n+2}]$$

from  $L_{m,n} = K^{m+n+2}$  such that  $(x)$  and  $[y]$  are incident if and only if relations from the written above list holds for variables

$\{x_1, x_2, x_3, x'_3, \dots, x_{n+2}, x'_{n+2}, x'_{n+3}, \dots, x'_{m+2}\} \cup \{y_1, y_2, y_3, y'_3, \dots, y_{m+2}, y'_{m+2}, y'_{m+3}, \dots, y'_{n+2}\}$ . We refer to written above list as list of variables of graph  $B(m, n, K)$ .

There is a natural homomorphism  $\phi_{m,n}$  from  $D(K)$  onto  $B(m, n, K)$  defined via procedure of deleting coordinates of infinite points  $(x)$  and lines  $[y]$  which do not belong to written above finite list.

If  $K = \mathbb{F}_q$  be the finite fields of  $q$  elements then  $B(m, n, K) = B(m, n, q)$ . We have the following results:

**PROPOSITION** *The projective limit of  $B(m, n, K) = B(m, n, q)$  if  $n \rightarrow \infty$  is an forest consisting of  $t = \lfloor m/2 \rfloor$  infinite  $q$ -regular trees.*

**THEOREM** *If  $m = cn + d$ ,  $c > 0$  then family of algebraic graphs  $B(m, n, q)$  is a  $q$ -regular bipartite almost Ramanujan graphs of large girth without edge transitive automorphism group.*

We define the colour  $\rho(v)$  of vertex  $v$  (point or line) from  $B(m, n, K)$  as first coordinate of corresponding tuple. For each vertex  $v$  of the graph  $B(m, n, K)$  there is exactly one neighbour  $N_\alpha(v)$  of colour  $\rho(v) + \alpha$  for chosen  $\alpha \in K$ . The map  $v \rightarrow N(v)$  is a bijection.

We can prove that all connected components of graphs  $B(m, n, K)$  are isomorphic. Let us denote by  $CB(m, n, K)$  the graph isomorphic to connected component of  $B(m, n, K)$ . Let  $N'_\alpha$  be the restriction of the operator  $N_\alpha$  onto the set of vertices of chosen connected component  $CB(m, n, K)$ . If  $\text{char}K \neq 2$  then connected component of the graph is the solution variety for the system of equations

$$\begin{aligned} a_1(v) &= b_1, \\ a_2(v) &= b_2, \\ &\dots \\ a_t(v) &= b_t. \end{aligned}$$

One can eliminate  $t = \lfloor m/2 \rfloor$  variables in operator  $N_\alpha$  using the above system of equations and this way determine the operator  $N'_\alpha$ . In our cryptographic algorithms we using this operators to increase the security.

## Keywords

multivariate cryptography, family of graphs of large girth, expanding graphs, Ramanujan graphs, regular trees via algebraic equations

## Bibliography

- [1] Ding J., Gower J. E., Schmidt D. S., *Multivariate Public Key Cryptosystems*, Springer, Advances in Information Security, 25 (XVIII) (2006): 260.
- [2] A. Lubotsky, R. Phillips, P. Sarnak, *Ramanujan graphs*, J. Comb. Theory., 115, N 2., (1989), 62-89.
- [3] F. Lazebnik, V. A. Ustimenko and A. J. Woldar, *A New Series of Dense Graphs of High Girth*, Bull (New Series) of AMS, v.32, N1, (1995), 73-79.
- [4] D. MacKay and M. Postol, *Weakness of Margulis and Ramanujan - Margulis Low Dencity Parity Check Codes*, Electronic Notes in Theoretical Computer Science, 74 (2003), 8pp.
- [5] G. Margulis, *Explicit group-theoretical constructions of combinatorial schemes and their application to desighn of expanders and concentrators*, Probl. Peredachi Informatzii., 24, N1, 51-60. English translation publ. Journal of Problems of Information transmission (1988), 39-46.
- [6] V. Ustimenko, *On the extremal graph theory for directed graphs and its cryptographical applications* In: T. Shaska, W.C. Huffman, D. Joener and V. Ustimenko, Advances in Coding Theory and Cryptography, Series on Coding and Cryptology, vol. 3, 181-200 (2007).
- [7] V. A. Ustimenko, U. Romańczuk, *On Extremal Graph Theory, Explicit Algebraic Constructions of Extremal Graphs and Corresponding Turing Encryption Machines*, in "Artificial Intelligence, Evolutionary Computing and Metaheuristics ", In the footsteps of Alan Turing Series: Studies in Computational Intelligence, Vol. 427, Springer, January, 2013, 257-285.

# Some remarks for codes and lattices over imaginary quadratic fields

Tony Shaska  
Oakland University, Rochester, MI, USA.

Caleb Shor  
Western New England University, Springfield, MA, USA.

shaska@oakland.edu

## Abstract

Let  $\ell > 0$  be a square-free integer,  $\ell \equiv 3 \pmod{4}$ ,  $K = \mathbb{Q}(\sqrt{-\ell})$ , and  $\mathcal{O}_K$  the ring of integers of  $K$ . Codes  $C$  over rings  $\mathcal{R} := \mathcal{O}_K/p\mathcal{O}_K$  determine lattices  $\Lambda_\ell(C)$  over  $K$ . The theta series  $\theta_{\Lambda_\ell(C)}$  of such lattice can be written in terms of the complete weight enumerator of  $C$ . For any  $\ell' > \ell$  the first  $\frac{\ell'+1}{4}$  terms of their corresponding theta functions are the same with those of  $\Lambda_{\ell'}(C)$ . In [6] it was conjectured that for  $\ell > \frac{p(n+1)(n+2)}{2}$  there is a unique complete weight enumerator corresponding to a given theta function. In this paper, we explore this conjecture and some new computational results.

## Keywords

Codes, theta functions, complete weight enumerators

## 1 Introduction

Let  $\ell > 0$  be a square-free integer congruent to 3 modulo 4,  $K = \mathbb{Q}(\sqrt{-\ell})$  be the imaginary quadratic field, and  $\mathcal{O}_K$  its ring of integers. Codes, Hermitian lattices, and their theta-functions over rings  $\mathcal{R} := \mathcal{O}_K/p\mathcal{O}_K$ , for small primes  $p$ , have been studied by many authors, see [1], [4], [5], among others. In [1], explicit descriptions of theta functions and MacWilliams identities are given for  $p = 2, 3$ . In [7] we explored codes  $C$  defined over  $\mathcal{R}$  for  $p > 2$ . For any  $\ell$  one can construct a lattice  $\Lambda_\ell(C)$  via Construction A and define theta functions based on the structure of the ring  $\mathcal{R}$ . Such constructions suggested some relations between the complete weight enumerator of the code and the theta function of the corresponding lattice. In this paper we further study the weight enumerators of such codes in terms of the theta functions of the corresponding lattices.

For any prime  $p$  with  $p \nmid \ell$ , let  $R := \mathcal{O}_K/p\mathcal{O}_K = \{a + b\omega : a, b \in \mathbb{F}_p, \omega^2 + \omega + d = 0\}$ , where  $d = (\ell + 1)/4$ . We have the map

$$\rho_{\ell,p} : \mathcal{O}_K \rightarrow \mathcal{O}_K/p\mathcal{O}_K =: \mathcal{R}$$

A linear code  $C$  of length  $n$  over  $\mathcal{R}$  is an  $\mathcal{R}$ -submodule of  $\mathcal{R}^n$ . The dual is defined as  $C^\perp = \{u \in \mathcal{R}^n : u \cdot \bar{v} = 0 \text{ for all } v \in C\}$ . If  $C = C^\perp$  then  $C$  is self-dual. We define

$$\Lambda_\ell(C) := \{u = (u_1, \dots, u_n) \in \mathcal{O}_K^n : (\rho_{\ell,p}(u_1), \dots, \rho_{\ell,p}(u_n)) \in C\},$$

In other words,  $\Lambda_\ell(C)$  consists of all vectors in  $\mathcal{O}_K^n$  in the inverse image of  $C$ , taken componentwise by  $\rho_{\ell,p}$ . This method of lattice construction is known as Construction A.

Let  $\tau \in \mathcal{H} = \{z \in \mathbb{C} : \text{Im}(z) > 0\}$ , the upper-half plane. And let  $q = e^{\pi i \tau}$ . For any lattice  $\Lambda$  in  $K^n$ , we have an associated theta function  $\theta_\Lambda(q)$ , given by

$$\theta_\Lambda(q) = \sum_{z \in \Lambda} q^{z \cdot \bar{z}},$$

where “ $\cdot$ ” denotes the usual dot product and  $\bar{z}$  denotes component-wise conjugation. Thus, for any linear code  $C$ , we have an associated lattice  $\Lambda_\ell(C)$  and associated theta function  $\theta_{\Lambda_\ell(C)}(q)$ .

For notation, let  $r_{a+pb+1} = a - b\omega$ , so  $\mathcal{R} = \{r_1, \dots, r_{p^2}\}$ . For a codeword  $u = (u_1, \dots, u_n) \in \mathcal{R}^n$  and  $r_i \in \mathcal{R}$ , we define the counting function  $n_i(u) := \#\{j : u_j = r_i\}$ . The complete weight enumerator of the  $\mathcal{R}$  code  $C$  is the polynomial

$$cwe_C(z_1, z_2, \dots, z_{p^2}) = \sum_{u \in C} z_1^{n_1(u)} z_2^{n_2(u)} \dots z_{p^2}^{n_{p^2}(u)}. \quad (1)$$

We can use the complete weight enumerator polynomial to find the theta function of the lattice  $\Lambda_\ell(C)$ . For a proof of the following result see [7].

**Lemma 1.** *Let  $C$  be a code defined over  $\mathcal{R}$  and  $cwe_C$  its complete weight enumerator as above. For integers  $a$  and  $b$  and a prime  $p$ , let  $\Lambda_{a,b}$  denote the lattice  $a - b\omega_\ell + p\mathcal{O}_K$ . Then,*

$$\theta_{\Lambda_\ell(C)}(q) = cwe_C(\theta_{\Lambda_{0,0}}(q), \theta_{\Lambda_{1,0}}(q), \dots, \theta_{\Lambda_{p-1,p-1}}(q)).$$

Note that the  $q^2$  arguments of this polynomial can be computed in terms of certain one-dimensional theta series which are defined in Section 2.1 of [7].

In [2], for  $p = 2$ , the symmetric weight enumerator polynomial  $swe_C$  of a code  $C$  over a ring or field of cardinality 4 is defined to be

$$swe_C(X, Y, Z) = cwe_C(X, Y, Z, Z).$$

For  $\Lambda_{\ell(C)}(q)$ , the lattice obtained from  $C$  by Construction A, by Theorem 5.2 of [2], one can then write

$$\theta_{\Lambda_\ell(C)}(q) = swe_C(\theta_{\Lambda_{0,0}}(q), \theta_{\Lambda_{1,0}}(q), \theta_{\Lambda_{0,1}}(q)).$$

These theta functions are referred to as  $A_d(q)$ ,  $C_d(q)$ , and  $G_d(q)$  in [2] and [8].

**Remark 1.** *The connection between complete weight enumerators of self-dual codes over  $\mathbb{F}_p$  and Siegel theta series of unimodular lattices is well known. Construction A associates to any length  $n$  code  $C = C^\perp$  an  $n$ -dimensional unimodular lattice; see [3] for details.*

For  $p > 2$ , however, there are  $\frac{(p+1)^2}{4}$  theta functions associated to the various lattices, so our analog of the symmetric weight enumerator polynomial needs more than 3 variables.

**Problem 1.** *Determine an explicit relation between theta functions and the symmetric weight enumerator polynomial of a code defined over  $\mathcal{R}$  for  $p > 3$ .*

We expect that the answer to the above problem is that the theta function is given as the symmetric weight enumerator  $swe_C$  of  $C$ , evaluated on the theta functions defined on cosets of  $\mathcal{O}_K/p\mathcal{O}_K$ .

## 2 Theta functions and the corresponding complete weight enumerator polynomials

For a fixed prime  $p$ , let  $C$  be a linear code over  $\mathcal{R} = \mathbb{F}_{p^2}$  or  $\mathbb{F}_p \times \mathbb{F}_p$  of length  $n$  and dimension  $k$ . An admissible level  $\ell$  is an integer  $\ell$  such that  $\mathcal{O}_K/p\mathcal{O}_K$  is isomorphic to  $\mathcal{R}$ . For an admissible  $\ell$ , let  $\Lambda_\ell(C)$  be the corresponding lattice as in the previous section. Then, the **level  $\ell$  theta function**  $\theta_{\Lambda_\ell(C)}(q)$  of the lattice  $\Lambda_\ell(C)$  is determined by the complete weight enumerator  $cwe_C$  of  $C$ , evaluated on the theta functions defined on cosets of  $\mathcal{O}_K/p\mathcal{O}_K$ . We consider the following questions. How do the theta functions  $\theta_{\Lambda_\ell(C)}(q)$  of the same code  $C$  differ for different levels  $\ell$ ? Can non-equivalent codes give the same theta functions for all levels  $\ell$ ?

We give a satisfactory answer to the first question (cf. Theorem 1, Lemma 2) and for the second question we conjecture that:

**Conjecture 1.** *Let  $C$  be a code of size  $n$  defined over  $\mathcal{R}$  and  $\theta_{\Lambda_\ell(C)}$  be its corresponding theta function for level  $\ell$ . Then, for large enough  $\ell$ , there is a unique complete weight enumerator polynomial which corresponds to  $\theta_{\Lambda_\ell(C)}$ .*

Let  $C$  be a code defined over  $\mathcal{R}$  for a fixed  $p > 2$ . Let the complete weight enumerator of  $C$  be the degree  $n$  polynomial  $cwe_C = f(x_1, \dots, x_r)$ , for  $r = p^2$ . Then from Lemma 1 we have that

$$\theta_{\Lambda_\ell(C)}(q) = f(\theta_{\Lambda_{0,0}}(q), \dots, \theta_{\Lambda_{p-1,p-1}}(q))$$

for a given  $\ell$ . First we want to address how  $\theta_{\Lambda_\ell(C)}(q)$  and  $\theta_{\Lambda_{\ell'}(C)}(q)$  differ for different  $\ell$  and  $\ell'$ .

**Theorem 1.** Let  $C$  be a code defined over  $\mathcal{R}$ . For all admissible  $\ell, \ell'$  with  $\ell < \ell'$  the following holds

$$\theta_{\Lambda_\ell(C)}(q) = \theta_{\Lambda_{\ell'}(C)}(q) + \mathcal{O}(q^{\frac{\ell+1}{4}}).$$

*Proof.* See [6] for details. □

We have the following lemma; see [6].

**Lemma 2.** Let  $C$  be a fixed code of size  $n$  defined over  $\mathcal{R}$  and  $\theta(q) = \sum \lambda_i q^i$  be its theta function for level  $\ell$ . Then, there exists a bound  $B_{\ell,p,n}$  such that  $\theta(q)$  is uniquely determined by its first  $B_{\ell,p,n}$  coefficients.

For notation, when  $p$  and  $n$  are fixed, we will let  $B_\ell = B_{\ell,p,n}$ . To extend the theory for  $p = 2$  to  $p > 2$  we have to find a relation between the theta function  $\theta_{\Lambda_\ell(C)}$  and the number of complete weight enumerator polynomials corresponding to it.

Fix an odd prime  $p$  and let  $C$  be a given code of length  $n$  over  $\mathcal{R}$ . Choose an admissible value of  $\ell$  such that there are  $\frac{(p+1)^2}{4}$  independent theta functions. Then, the complete weight enumerator of  $C$  has degree  $n$  and  $r = \frac{(p+1)^2}{4}$  variables  $x_1, \dots, x_r$ . We call a **generic complete weight enumerator polynomial** a homogeneous polynomial  $P \in \mathbb{Q}[x_1, \dots, x_r]$ .

Denote by  $P(x_1, \dots, x_r)$  a generic  $r$ -nary, degree  $n$ , homogeneous polynomial. Assume that there is a length  $n$  code  $C$  defined over  $\mathcal{R}$  such that  $P(x_1, \dots, x_r)$  is the symmetric weight enumerator polynomial. In other words,

$$swe_C(x_1, \dots, x_r) = P(x_1, \dots, x_r)$$

Fix the level  $\ell$ . Then, by replacing

$$x_1 = \theta_{\Lambda_{0,0}}(q), \dots, x_r = \theta_{\Lambda_{p-1,p-1}}(q),$$

we compute the left side of the above equation as a series  $\sum_{i=0}^{\infty} \lambda_i q^i$ . By equating both sides of  $\sum_{i=0}^{\infty} \lambda_i q^i = P(x_1, \dots, x_r)$ , we can get a linear system of equations. Since the first  $\lambda_0, \dots, \lambda_{B_\ell-1}$  determine all the coefficients of the theta series then we have to pick  $B_\ell$  equations (these equations are not necessarily independent).

Consider the coefficients of the polynomial  $P(x_1, \dots, x_r)$  as parameters  $c_1, \dots, c_s$ . Then, the linear map

$$\begin{aligned} L_\ell : \mathbb{C}^s &\rightarrow \mathbb{C}^{B_\ell-1} \\ (c_1, \dots, c_s) &\mapsto (\lambda_0, \dots, \lambda_{B_\ell-1}) \end{aligned}$$

has an associated matrix  $M_\ell$ . For a fixed value of  $(\lambda_0, \dots, \lambda_{B_\ell-1})$ , determining the rank of the matrix  $M_\ell$  would determine the number of polynomials giving the same theta series. There is a unique complete weight enumerator corresponding to a given theta function when

$$\text{null}(M_\ell) = s - \text{rank}(M_\ell) = 0$$

**Conjecture 2.** For  $\ell \geq \frac{p(n+1)(n+2)}{n} - 1$  we have  $\text{null} M_\ell = 0$ , or in other words

$$\text{rank}(M_\ell) = \frac{\left(n - 1 + \frac{(p+1)^2}{4}\right)!}{n! \cdot \left(\frac{(p+1)^2}{4} - 1\right)!}$$

The choice of  $\ell$  is taken from experimental results for primes  $p = 2$  and  $3$ . More details are given in the next section.

It is obvious that Conjecture 2 implies Conjecture 1. If Conjecture 1 is true then for large enough  $\ell$  there would be a one to one correspondence between the complete weight enumerator polynomials and the corresponding theta functions. Perhaps, more interesting is to find  $\ell$  and  $p$  for which there is not a one to one such correspondence. Consider the map

$$\Phi(\ell, p) = (\lambda_0(\ell, p), \dots, \lambda_{B_\ell-1}(\ell, p)),$$

where  $\lambda_0, \dots, \lambda_{B_\ell-1}$  are now functions in  $\ell$  and  $p$ . Let  $V$  be the variety given by the Jacobian of the map  $\Phi$ . Finding integer points  $\ell, p$  on this variety such that  $\ell$  and  $p$  satisfy our assumptions would give us values for  $\ell, p$  when the above correspondence is not one to one. However, it seems quite hard to get explicit description of the map  $\Phi$ . Next, we will try to shed some light over the above conjectures for fixed small primes  $p$ .

### 3 Bounds for small primes

In [8] we determine explicit bounds for the above theorems for prime  $p = 2$ . In this section we give some computation evidence for the generalization of the result for  $p = 3$ . We recall the theorem for  $p = 2$ .

**Theorem 2** ([8], Thm. 2). *Let  $p = 2$  and  $C$  be a code of size  $n$  defined over  $\mathcal{R}$  and  $\theta_{\Lambda_\ell}(C)$  be its corresponding theta function for level  $\ell$ . Then the following hold:*

- i) *For  $\ell < \frac{2(n+1)(n+2)}{n} - 1$  there is a  $\delta$ -dimensional family of symmetrized weight enumerator polynomials corresponding to  $\theta_{\Lambda_\ell}(C)$ , where*  

$$\delta \geq \frac{(n+1)(n+2)}{2} - \frac{n(\ell+1)}{4} - 1.$$
- ii) *For  $\ell \geq \frac{2(n+1)(n+2)}{n} - 1$  and  $n < \frac{\ell+1}{4}$  there is a unique symmetrized weight enumerator polynomial which corresponds to  $\theta_{\Lambda_\ell}(C)$ .*

These results were obtained by using the explicit expression of theta in terms of the symmetric weight enumerator valuated on the theta functions of the cosets.

Next we want to find explicit bounds for  $p = 3$  as in the case of  $p = 2$ . In the case of  $p = 3$  it is enough to consider four theta functions,  $\theta_{\Lambda_{0,0}}(q)$ ,  $\theta_{\Lambda_{1,0}}(q)$ ,  $\theta_{\Lambda_{0,1}}(q)$ , and  $\theta_{\Lambda_{1,1}}(q)$  since  $\theta_{\Lambda_{2,0}}(q) = \theta_{\Lambda_{1,0}}(q)$ ,  $\theta_{\Lambda_{2,2}}(q) = \theta_{\Lambda_{1,1}}(q)$  and  $\theta_{\Lambda_{0,2}}(q) = \theta_{\Lambda_{1,2}}(q) = \theta_{\Lambda_{2,1}}(q) = \theta_{\Lambda_{0,1}}(q)$ . If we are given a code  $C$  and its weight enumerator polynomial then we can find the theta function of the lattice constructed from  $C$  using Construction A. Let  $\theta(q) = \sum_{i=0}^{\infty} \lambda_i q^i$  be the theta series for level  $\ell$  and

$$p(x, y, z, w) = \sum_{i+j+k+m=n} c_{i,j,k} x^i y^j z^k w^m$$

be a degree  $n$  generic 4-nary homogeneous polynomial. We would like to find out how many polynomials  $p(x, y, z, w)$  correspond to  $\theta(q)$  for a fixed  $\ell$ . For a given  $\ell$  find  $\theta_{\Lambda_{0,0}}(q)$ ,  $\theta_{\Lambda_{1,0}}(q)$ ,  $\theta_{\Lambda_{0,1}}(q)$  and  $\theta_{\Lambda_{1,1}}(q)$  and substitute them in the  $p(x, y, z, w)$ . Hence,  $p(x, y, z, w)$  is now written as a series in  $q$ . We get infinitely many equations by equating the corresponding coefficients of the two sides of the equation

$$p(\theta_{\Lambda_{0,0}}(q), \theta_{\Lambda_{1,0}}(q), \theta_{\Lambda_{0,1}}(q), \theta_{\Lambda_{1,1}}(q)) = \sum_{i=0}^{\infty} \lambda_i q^i.$$

Since the first  $\lambda_0, \dots, \lambda_{B_\ell-1}$  determine all the coefficients of the theta series then it is enough to pick the first  $B_\ell$  equations. The linear map

$$L_\ell : (c_1, \dots, c_{20}) \mapsto (\lambda_0, \dots, \lambda_{B_\ell-1})$$

has an associated matrix  $M_\ell$ . If the nullity of  $M_\ell$  is zero then we have a unique polynomial that corresponds to the given theta series. We have calculated the nullity of the matrix and  $B_\ell$  for small  $n$  and  $\ell$ .

**Example 1** (The case  $p = 3, n = 3$ ). *The generic homogenous polynomial is given by*

$$\begin{aligned} P(x, y, z) = & c_1 x^3 + c_2 x^2 y + c_3 x^2 z + c_4 x^2 w + c_5 x y^2 + c_6 x z^2 + c_7 x w^2 + c_8 x y z \\ & + c_9 x y w + c_{10} x z w + c_{11} y^3 + c_{12} y^2 z + c_{13} y^2 w + c_{14} y z^2 + c_{15} y w^2 \\ & + c_{16} y z w + c_{17} z^3 + c_{18} z^2 w + c_{19} z w^2 + c_{20} w^3. \end{aligned} \quad (2)$$

*The system of equations can be written by the form of*

$$A\vec{c} = \vec{\lambda}$$

*where  $\vec{c} = (c_1 \ c_2 \ \dots \ c_{20})^t$ ,  $\vec{\lambda} = (\lambda_0 \ \lambda_1 \ \dots \ \lambda_{15})^t$ . In the case of  $\ell = 7$  the matrix  $M_7$  has null  $(M_7) = 4$ . We have a positive dimension family of solution set. The case of  $\ell = 11$  the matrix  $M_{11}$  has null  $(M_{11}) = 1$ . For any case where  $\ell \geq 19$  the nullity of the matrix is 0. Hence, for every given theta series, there is a unique symmetric weight enumerator polynomial. .*

We summarize the results in the following table:

$\ell$	$n = 3$		$n = 4$		$n = 5$	
	$B_\ell$	$\text{null } M_\ell$	$B_\ell$	$\text{null } M_\ell$	$B_\ell$	$\text{null } M_\ell$
7	16	4	26	9	33	24
11	19	1	30	5	42	14
19	22	0	38	0	60	0
23	25	0	37	0	58	0
31	31	0	41	0	60	0
35	34	0	48	0	61	0
43	40	0	55	0	69	0
47	43	0	60	0	74	0
55	49	0	70	0	86	0
59	52	0	75	0	92	0

Recall that  $\ell \equiv 3 \pmod{4}$  and  $p \nmid \ell$ . It seems from the table that the same bound of  $B_\ell = \frac{2(n+1)(n+2)}{n}$  as for  $p = 2$  holds also for  $p = 3, n = 3$ .

We have the following conjecture for general  $p, n$  and  $\ell$ .

**Conjecture 3.** *For a given theta function  $\theta_{\Lambda_\ell(C)}$  of a code  $C$  for level  $\ell$  there is a unique complete weight enumerator polynomial corresponding to  $\theta_{\Lambda_\ell(C)}$  if  $\ell \geq \frac{p(n+1)(n+2)}{n}$ .*

It is interesting to consider such question for such lattices independently of the connection to coding theory. What is the meaning of the bound  $B_\ell$  for the ring  $\mathcal{O}_K/p\mathcal{O}_K$ ? Do the theta functions defined here correspond to any modular forms? Is there any difference between the cases when the ring is  $\mathbb{F}_p \times \mathbb{F}_p$  or  $\mathbb{F}_{p^2}$ ?

## References

- [1] C. Bachoc, Applications of coding theory to the construction of modular lattices. *J. Combin. Theory Ser. A* 78 (1997), no. 1, 92–119.
- [2] K. S. Chua, Codes over  $\text{GF}(4)$  and  $\mathbf{F}_2 \times \mathbf{F}_2$  and Hermitian lattices over imaginary quadratic fields. *Proc. Amer. Math. Soc.* 133 (2005), no. 3, 661–670 (electronic).
- [3] J. Leech and N. J. A. Sloane, Sphere packing and error-correcting codes, *Canadian J. Math.*, **23**, (1971), 718-745.
- [4] F. J. MacWilliams, N. J. A. Sloane, The theory of error-correcting codes. II. North-Holland Mathematical Library, Vol. 16. North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977. pp. i–ix and 370–762.
- [5] F. J. MacWilliams, N. J. A. Sloane, The theory of error-correcting codes. I. North-Holland Mathematical Library, Vol. 16. North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977. pp. i–xv and 1–369.
- [6] T. Shaska, C. Shor, C. S. Wijesiri, Codes over rings of size  $p^2$  and lattices over imaginary quadratic fields. *Finite Fields Appl.* 16 (2010), no. 2, 7587.
- [7] T. Shaska and C. Shor, Codes over  $F_{p^2}$  and  $F_p \times F_p$ , lattices, and corresponding theta functions. *Advances in Coding Theory and Cryptology*, vol 3. (2007), pg. 70-80.
- [8] T. Shaska and S. Wijesiri, Codes over rings of size four, Hermitian lattices, and corresponding theta functions, *Proc. Amer. Math. Soc.*, 136 (2008), 849-960.
- [9] T. Shaska and C. Shor, Theta functions and complete weight enumerators for codes over imaginary quadratic fields, (work in progress).



# An Efficient Algorithm for Computing Branch Gröbner Systems and Its Applications in Algebraic Cryptanalysis

Yao Sun, Zhenyu Huang, Dongdai Lin  
SKLOIS, Institute of Information Engineering, CAS, (China)

Dingkang Wang  
KLMM, Academy of Mathematics and Systems Science, CAS, (China)

dwang@mmrc.iss.ac.cn

## Abstract

Solving systems of boolean polynomial equations is a kernel problem in algebraic computations and Gröbner basis is one of the most important tools to solve such systems.

In 2009, Sun and Wang proposed an algorithm for computing a branch Gröbner system [8, 9] based on the matrix version of the F5 algorithm [4]. For a set of boolean polynomials, their algorithm uses the F5 algorithm to compute a Gröbner basis, and creates branches before constructing huge matrices, such that the computing complexity for each branch can be controlled in a relative low level. Their algorithm uses zero-suppressed binary decision diagrams (ZDD) to store Boolean polynomials and has a good performance for a class of stream cypher generated by linear feedback shift registers. The ZDD data structure is also used in PolyBoRi [1] and Chai et al.'s characteristic set algorithm [3, 5].

In this talk, a new algorithm for computing branch Gröbner systems is presented. Some new techniques for manipulating boolean polynomials are used to build Gröbner bases for all branches. ZDD is again used as the basic data structure to store boolean polynomials. The implementation of this new algorithm in C performs very well for many examples. The ideas used in this new algorithm can also be extended to compute branch Gröbner systems in a more general form, which will be studied in our future work.

Let  $B := \mathbb{F}_2[x_1, \dots, x_n]/\langle x_1^2 - x_1, \dots, x_n^2 - x_n \rangle$  be a boolean polynomial ring over the binary field  $\mathbb{F}_2 = \{0, 1\}$  with  $n$  variables  $\{x_1, \dots, x_n\}$ . Let  $F$  be a set of boolean polynomials in  $B$ , an ideal generated by  $F$  over  $B$  is defined as  $\langle F \rangle = \{p_1 f_1 + \dots + p_m f_m \mid p_1, \dots, p_m \in B, f_1, \dots, f_m \in F\}$ .

Let  $\prec$  be an order on  $B$  deduced from a monomial order in  $\mathbb{F}_2[x_1, \dots, x_n]$ , and  $F$  be a set of boolean polynomials in  $B$ . A set  $G \subset \langle F \rangle$  is called a **Gröbner basis** of  $\langle F \rangle$ , if for any  $f \in \langle F \rangle$ , there exists  $g \in G$  such that  $\text{lm}(g)$  divides  $\text{lm}(f)$ .

In this talk, we will consider a variant of Gröbner bases.

**Definition 1 (Branch Gröbner system)** Let  $\prec$  be an order on  $B$  deduced from a monomial order in  $\mathbb{F}_2[x_1, \dots, x_n]$ , and  $F$  be a set of boolean polynomials in  $B$ . A finite set  $\mathcal{G} = \{G_1, \dots, G_l\}$  is called a **branch Gröbner system** of the ideal  $\langle F \rangle$ , if

1.  $G_i$  is a Gröbner basis for the ideal  $\langle G_i \rangle \subset B$ , and
2.  $V(F) = V(G_1) \cup \dots \cup V(G_l)$ ,

where  $V(F) = \{\alpha \in \mathcal{F}_2^n \mid f(\alpha) = 0, \forall f \in F\}$  and similarly for  $V(G_i)$ . Particularly, each  $G_i$  is called a branch of this branch Gröbner system  $\mathcal{G}$ .

Please note that a general Gröbner basis of  $\langle F \rangle$  directly constructs a branch Gröbner system. A branch Gröbner system will be easier to be computed than a general Gröbner basis, because in each branch the corresponding system is simpler. In current talk, instead of computing a branch Gröbner system in its general form, we present an efficient algorithm for computing a special branch Gröbner system defined below.

**Definition 2 (Linear branch Gröbner system)** A branch Gröbner system  $\mathcal{G} = \{G_1, \dots, G_l\}$  is called a **linear branch Gröbner system** of the ideal  $\langle F \rangle$ , if for any  $g \in G_i$ , we have  $\text{lm}(g) \in \{x_1, \dots, x_n\}$  where  $i = 1, \dots, l$ , i.e. each polynomial appearing in this branch Gröbner system has a linear leading monomial.

Linear branch Gröbner systems are similar to the characteristic sets discussed in [3, 5]. But the algorithm presented in this paper can be extended to compute other branch Gröbner systems with a small adaption.

Clearly, a linear branch Gröbner system is sufficient to find all points in  $V(F)$  directly.

The new algorithm has been implemented in C based on the CUDD package [7]. Our implementation is tested by the famous Bivium stream cipher after guessing several bits. Examples are from [6], and the input of examples all include 176 variables and 160 polynomials. The timing below is obtained from a PC (Core i7-2600, 4GB memory) running Windows 7 (64 bit).

Table 1: Timings (sec.)

Bits guessed	Average Time	Max Time	Min Time
37	0.186	0.359	0.078
36	0.401	0.609	0.265
35	0.655	0.874	0.453
34	3.584	9.391	1.342

In the above table, the first column shows how many bits/variables are guessed in the Bivium system. Average Time is obtained from 10 times of *arbitrary* guesses. Max Time and Min Time give the largest and smallest time during these tests. The data in this table shows this new algorithm is efficient and guessing 35 variables leads to the best attack of Bivium system which is consistent with existing results.

### Keywords

Gröbner basis, branch Gröbner system, boolean polynomial, algorithm, algebraic cryptanalysis.

## References

- [1] M. Brickenstein and A. Dreyer. PolyBoRi: A framework for Gröbner-basis computations with Boolean polynomials. *J. Symb. Comp.*, vol. 44(9), 1326-1345, 2009.
- [2] Raddum, H.: Cryptanalytic results on TRIVIUM. eSTREAM, ECRYPT Stream Cipher Project, Report 2006/039 (2006)
- [3] F.J. Chai, X.S. Gao, and C.M. Yuan. A characteristic set method for solving Boolean equations and applications in cryptanalysis of stream ciphers. *J. Syst. Sci. Complex.*, vol. 21(2), 191-208, 2008.
- [4] J.-C. Faugère. A new efficient algorithm for computing Gröbner bases without reduction to zero ( $F_5$ ). In *Proc. ISSAC'02*, ACM Press, 75-82, 2002. Revised version downloaded from [fgbrs.lip6.fr/jcf/Publications/index.html](http://fgbrs.lip6.fr/jcf/Publications/index.html).
- [5] X.S. Gao and Z.Y. Huang. Characteristic set algorithms for equation solving in finite fields. *J. Symb. Comp.*, vol. 47(6), 655-679, 2012.
- [6] Z.Y. Huang and D.D. Lin. Attacking Bivium and Trivium with the Characteristic Set method. *AFRICACRYPT 2011*, 77-91, 2011.
- [7] F. Somenzi. CUDD: CU Decision Diagram package release 2.3.0. University of Colorado at Boulder, 1998.
- [8] Y. Sun and D.K. Wang. Branch Gröbner bases algorithm over Boolean ring (in Chinese). *J. Syst. Sci. & Math. Sci.*, vol. 9, 1266-1277, 2009.
- [9] Y. Sun and D.K. Wang. The implementation and complexity analysis of the branch Gröbner bases algorithm over Boolean ring. In *Proc. ASCM 2009*, 191-200, 2009.

# On some algebraic aspects of data security in cloud computing

Vasyl Ustimenko, Aneta Wroblewska  
Maria Curie-Skłodowska University in Lublin (Poland)

awroblewska@hektor.umcs.lublin.pl

## Abstract

The paper is dedicated to ideas of homomorphic encryption and multivariate key dependent cryptography. We observe recent theoretical results on the above-mentioned topics together with their applications to cloud security. Post Quantum Cryptography could not use many security tools based on Number Theory, because of the factorization algorithm developed by Peter Shor. This fact and fast development of Computer Algebra make multivariate cryptography an important direction of research. The idea of key dependent cryptography looks promising for applications in Clouds, because the size of the key allows to control the speed of execution and security level. Finally, special classes of finite rings turned out to be very useful in homomorphic encryption and for the development of multivariate key.

Cloud computing provides clients with a virtual computing infrastructure on top of which they can store data and run applications. While the benefits of cloud computing are clear, it introduces new security challenges since cloud operators are expected to manipulate client data without necessarily being fully trusted. We are designing cryptographic primitives and protocols tailored to the setting of cloud computing, attempting to strike a balance between security, efficiency and functionality. The current generation of cloud storage services do not provide any security against untrusted cloud operators making them unsuitable for storing sensitive information such as medical records, financial records or high impact business data. To address this we are pursuing various research projects that range from theory to practice.

**Homomorphic encryption.** The most common use of encryption is to provide confidentiality by hiding all useful information about the plaintext. Encryption, however, renders data useless in the sense that one loses the ability to operate on it. To address this we are designing cryptosystems that support a variety of computations on encrypted data, ranging from general-purpose computations (i.e., fully-homomorphic encryption) to special-purpose computations (e.g., voting and search).

**Searchable structured encryption.** A searchable encryption scheme encrypts data in such a way that a token can be generated to allow a third party to search over the encrypted data. Using a searchable encryption scheme, a client can safely store its data with an untrusted cloud provider without losing the ability to search over it. There is a need of structured encryption which allows a client to encrypt various types of data (e.g., social networks or web graphs) in such a way that complex queries can be performed over the encrypted data. Structured encryption and various constructions for graph data is known.

Some security issues raised by cloud computing are motivated by virtualization. Dynamic scalability or elasticity will help generalize high-performance computing and very large data sets in applications. But the real gains in performance depend heavily on the predictability of physical and virtualized resources. It means that the balancing of performance against security and the adaptation of HPC or VLDB techniques to cloud computing are important issues and will have long-lasting scientific content. The direction of Key Dependent Message (KDM) secure encryption in Cryptography can bring an appropriate security tools for Cloud Computing.

The goal of the presented paper is discussion of new KDM cryptosystems, which have some potential to be used in the era of Postquantum Cryptography. The Quantum Computer is a special random computational machine. Recall that computation in Turing machine can be formalised with the concept of finite automaton as a walk in the graph with arrows labelled by special symbols. "Random computation" can be defined as a random walk in the random graph. So we are looking for the deterministic approximation of random graphs by extremal algebraic graphs. It is known that the explicit solutions for an optimization graphs have properties similar to random graphs. The probability of having rather short cycle in the walking process on random graph is zero. So the special direction of Extremal Graph Theory

of studies of graphs of order  $v$  (the variable) without short cycles of maximal size (number of edges) can lead to the discovery of good approximation for random graphs.

### Keywords

multivariate cryptography, cloud computing, symbolic computations, graphs of large girth

## 1 Introduction

The plainspace of the algorithm is  $K^n$ , where  $K$  is the chosen commutative ring. Graph theoretical encryption corresponds to walk on the bipartite graph with partition sets which are isomorphic to  $K^n$ . We conjugate chosen graph based encryption map, which is a composition of several elementary polynomial automorphisms of a free module  $K^n$  with special invertible affine transformation of  $K^n$ . Finally we compute symbolically the corresponding polynomial map  $g$  of  $K^n$  onto  $K^n$ . We say that the sequence  $g_n, n \geq 3, n \rightarrow \infty$  of polynomial transformation bijective maps of free module  $K^n$  over commutative ring  $K$  is a sequence of stable degree if the order of  $g_n$  is growing with  $n$  and the degree of each nonidentical polynomial map of kind  $g_n^k$  is an independent constant  $c$ . A transformation  $b = \tau g_n^k \tau^{-1}$ , where  $\tau$  is affine bijection,  $n$  is large and  $k$  is relatively small, can be used as a base of group theoretical Diffie-Hellman key exchange algorithm for the Cremona group  $C(K^n)$  of all regular automorphisms of  $K^n$ . The specific feature of this method is that the order of the base may be unknown for the adversary because of the complexity of its computation. The exchange can be implemented by tools of Computer Algebra (symbolic computations). The adversary can not use the degree of righthandside in  $b^x = d$  to evaluate unknown  $x$  in this form for the discrete logarithm problem.

In the paper we introduce the explicit constructions of sequences of elements of stable degree  $c$  for each commutative ring  $K$  containing at least 3 elements and each  $c \geq 2$ . Special cases of  $c = 3$  and  $c = 2$  were obtained in [11] and [10]. We discuss the implementation of related key exchange and public key algorithms. It is interesting that in the case of  $c \geq 4$  use of special affine bijections lead to sparse polynomial transformation with  $O(n^3)$  monomial expressions. Those results are based on the construction of the family  $D(n, q)$  of graphs with large girth and the description of their connected components  $CD(n, q)$ . The existence of infinite families of graphs of large girth had been proven by Paul Erdős' (see [1]). Together with famous Ramanujan graphs introduced by G. Margulis [4] and investigated in [3] graphs  $CD(n, q)$  is one of the first explicit constructions of such a families with unbounded degree. Graphs  $D(n, q)$  had been used for the construction of LDPS codes and turbocodes which were used in real satellite communications ([2]), for the development of private key encryption algorithms ([9], [5]), the option to use them for public key cryptography was considered in [8], [7] and in [6], where the related dynamical system had been introduced.

## 2 Preliminaries

Let  $\mathbb{K}$  denote commutative ring.

Set  $Q$  of the ring  $\mathbb{K}$  is **the multiplicative set** of ring  $\mathbb{K}$ , if it is closed under operation of multiplication ( $x, y \in Q \Rightarrow x \cdot y \in Q$ ) and does not contain 0.

Elements  $t_1, t_2, \dots, t_l, l \geq 1 \in \mathbb{K}$  are called **multiplicative generators**, if there is a multiplicative set  $Q$  containing all  $t_i, i = 1, 2, \dots, l$ .

### 2.1 Graphs and incidence system

The missing definitions of graph-theoretical concepts which appear in this paper can be found in [1]. All graphs we consider are simple, i.e. undirected without loops and multiple edges. Let  $V(G)$  and  $E(G)$  denote the set of vertices and the set of edges of  $G$ , respectively. Then  $|V(G)|$  is called the *order* of  $G$ , and  $|E(G)|$  is called the *size* of  $G$ . A path in  $G$  is called *simple* if all its vertices are distinct. When it is convenient, we shall identify  $G$  with the corresponding anti-reflexive binary relation on  $V(G)$ , i.e.  $E(G)$  is a subset of  $V(G) \times V(G)$  and write  $vGu$  for the adjacent vertices  $u$  and  $v$  (or neighbors). The sequence of distinct vertices  $v_1, \dots, v_t$ , such that  $v_i G v_{i+1}$  for  $i = 1, \dots, t-1$  is the pass in the graph. The length of a pass is a number of its edges. The distance  $\text{dist}(u, v)$  between two vertices is the length of the shortest pass between them. The diameter of the graph is the maximal distance between two vertices  $u$  and  $v$  of the graph. Let  $C_m$  denote the cycle of length  $m$  i.e. the sequence of distinct vertices  $v_1, \dots, v_m$  such that  $v_i G v_{i+1}$ ,

$i = 1, \dots, m-1$  and  $v_m G v_1$ . The girth of a graph  $G$ , denoted by  $g = g(G)$ , is the length of the shortest cycle in  $G$ . The degree of vertex  $v$  is the number of its neighbors (see [15] or [1]).

The incidence structure is the set  $V$  with partition sets  $P$  (points) and  $L$  (lines) and symmetric binary relation  $I$  such that the incidence of two elements implies that one of them is a point and another is a line. We shall identify  $I$  with the simple graph of this incidence relation (bipartite graph). If number of neighbours of each element is finite and depends only on its type (point or line), then the incidence structure is a tactical configuration in the sense of Moore (see [12]). The graph is  $k$ -regular if each of its vertex has degree  $k$ , where  $k$  is a constant. In this section we reformulate results of [13], [14] where the  $q$ -regular tree was described in terms of equations over finite field  $F_q$ .

Let  $q$  be a prime power, and let  $P$  and  $L$  be two countably infinite dimensional vector spaces over  $F_q$ . Elements of  $P$  will be called *points* and those of  $L$  *lines*. To distinguish points from lines we use parentheses and brackets: If  $x \in V$ , then  $(x) \in P$  and  $[x] \in L$ . It will also be advantageous to adopt the notation for coordinates of points and lines introduced in [4]:

$$(p) = (p_1, p_{11}, p_{12}, p_{21}, p_{22}, p'_{22}, p_{23}, \dots, p_{ii}, p'_{ii}, p_{i,i+1}, p_{i+1,i}, \dots),$$

$$[l] = [l_1, l_{11}, l_{12}, l_{21}, l_{22}, l'_{22}, l_{23}, \dots, l_{ii}, l'_{ii}, l_{i,i+1}, l_{i+1,i}, \dots).$$

We now define an incidence structure  $(P, L, I)$  as follows. We say the point  $(p)$  is incident with the line  $[l]$ , and we write  $(p)I[l]$ , if the following relations between their coordinates hold:

$$\begin{aligned} l_{11} - p_{11} &= l_1 p_1 \\ l_{12} - p_{12} &= l_{11} p_1 \\ l_{21} - p_{21} &= l_1 p_{11} \\ l_{ii} - p_{ii} &= l_1 p_{i-1,i} \\ l'_{ii} - p'_{ii} &= l_{i,i-1} p_1 \\ l_{i,i+1} - p_{i,i+1} &= l_{ii} p_1 \\ l_{i+1,i} - p_{i+1,i} &= l_1 p'_{ii} \end{aligned} \tag{1}$$

(The last four relations in (1) are defined for  $i \geq 2$ .) This incidence structure  $(P, L, I)$  we denote as  $D(q)$ . We speak now of the *incidence graph* of  $(P, L, I)$ , which has the vertex set  $P \cup L$  and edge set consisting of all pairs  $\{(p), [l]\}$  for which  $(p)I[l]$ .

## 2.2 Connected components

Let us consider the description of connected components of the graphs.

Let  $n \geq 6$ ,  $t = \lfloor (n+2)/4 \rfloor$ , and let  $u = (u_1, u_{11}, \dots, u_{tt}, u'_{tt}, u_{t,t+1}, u_{t+1,t}, \dots)$  be a vertex of  $D(n, \mathbb{K})$ . (It does not matter whether  $u$  is a point or a line). For every  $r$ ,  $2 \leq r \leq t$ , let

$$a_r = a_r(u) = \sum_{i=0}^r (u_{ii} u'_{r-i, r-i} - u_{i, i+1} u_{r-i, r-i-1}) \tag{2}$$

and  $a = a(u) = (a_2, a_3, \dots, a_t)$ . (Here we define

$$p_{-1,0} = l_{0,-1} = p_{1,0} = l_{0,1} = 0, p_{00} = l_{00} = -1, p_{0,1} = p_1, l_{1,0} = l_1, p'_{00} = l'_{00} = 1, l'_{11} = l_{11}, p'_{1,1} = p_{1,1}).$$

In [13] the following statement was proved.

**Proposition 1** *Let  $u$  and  $v$  be vertices from the same component of  $D(k, q)$ . Then  $a(u) = a(v)$ . Moreover, for any  $t-1$  field elements  $x_i \in F_q$ ,  $2 \leq t \leq \lfloor (k+2)/4 \rfloor$ , there exists a vertex  $v$  of  $D(k, q)$  for which*

$$a(v) = (x_2, \dots, x_t) = (x).$$

**Corollary 1** *Let us consider a general vertex*

$$x = (x_1, x_{1,1}, x_{2,1}, x_{1,2}, \dots, x_{i,i}, x'_{i,i}, x_{i+1,i}, x_{i,i+1}, \dots),$$

$i = 2, 3, \dots$  of the connected component  $CD(n, \mathbb{K})$ , which contains a chosen vertex  $v$ . Then, coordinates  $x_{i,i}$ ,  $x_{i,i+1}$ ,  $x_{i+1,i}$  can be chosen independently as "free parameters" from  $\mathbb{K}$  and  $x'_{i,i}$  could be computed successively as the unique solution of the equations  $a_i(x) = a_i(v)$ ,  $i = 2, 3, \dots$

### 3 Operators $L_{D,n,\beta_k}$ and $P_{D,n,\alpha_k}$

Let  $L_{D,n,\beta_k}$  be the operator of taking the neighbour of point:

$$(p)^{2k-2} = (p_{0,1}, p_{1,1}, p_{1,2}, p_{2,1}, p_{2,2}, p'_{2,2}, p_{2,3}, \dots, p_{i,i}, p'_{i,i}, p_{i,i+1}, p_{i+1,i}, \dots),$$

of a kind

$$[l]^{2k-1} = [\beta_k, l_{1,1}, l_{1,2}, l_{2,1}, l_{2,2}, l'_{2,2}, l_{2,3}, \dots, l_{i,i}, l'_{i,i}, l_{i,i+1}, l_{i+1,i}, \dots],$$

where parameters  $l_{1,1}, l_{1,2}, l_{2,1}, l_{2,2}, \dots, l_{i,i}, l_{i,i+1}, l_{i+1,i}, \dots$  are computed consequently from the equations (1) in definition of  $D(n, \mathbb{K})$  and all  $l'_{i,i}$  for  $i = 2, 3, \dots$  are computed using equation describing connected component (2).

Similarly,  $P_{D,n,\alpha_k}$  is the operator of taking the neighbour of line

$$[l]^{2k-1} = [l_{1,0}, l_{1,1}, l_{1,2}, l_{2,1}, l_{2,2}, \dots, l_{i,i}, l_{i,i+1}, l'_{i,i}, l_{i+1,i}, \dots],$$

of a kind

$$(p)^{2k} = (p_{0,1}^{2k-2} + \alpha_k, p_{1,1}, p_{1,2}, p_{2,1}, p_{2,2}, \dots, p_{i,i}, p'_{i,i}, p_{i,i+1}, p_{i+1,i}, \dots),$$

where parameters  $p_{1,1}, p_{1,2}, p_{2,1}, p_{2,2}, \dots, p_{i,i}, p_{i,i+1}, p_{i+1,i}, \dots$  are computed consequently from the equations (1) in definition of  $D(n, \mathbb{K})$  and all  $p'_{i,i}$  for  $i = 2, 3, \dots$  are computed using equation describing connected component (2).

Given the vector  $(p)^0 = (p_{0,1}, p_{1,1}, p_{1,2}, p_{2,1}, p_{2,2}, p'_{2,2}, p_{2,3}, \dots, p_{i,i}, p'_{i,i}, p_{i,i+1}, p_{i+1,i}, \dots)$ , (of length  $n$ ) let us take elements  $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_k)$  and  $\beta = (\beta_1, \beta_2, \dots, \beta_k)$  from  $Q^k$  and composition  $F_{n,\alpha,\beta} = L_{D,n,\beta_1} P_{D,n,\alpha_1} L_{D,n,\beta_2} P_{D,n,\alpha_2} \dots L_{D,n,\beta_k} P_{D,n,\alpha_k}$ .

**Theorem 1** (*A. Wroblewska*) *Independently from the choice of  $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_k) \in Q^k$  and  $\beta = (\beta_1, \beta_2, \dots, \beta_k) \in Q^k$ , the map  $F_{n,\alpha,\beta}$  of free module  $\mathbb{K}^{n - \lfloor \frac{n+2}{4} \rfloor}$  is bijective map with degree  $\lfloor \frac{n+2}{4} \rfloor$ .*

**Theorem 2** (*V. Ustimenko*) *The order  $F_{n,\alpha,\beta}$  is going to  $\infty$  when  $n \rightarrow \infty$*

## 4 Application

### 4.1 Public key algorithm

Let  $\tau$  be linear transformation  $\tau : x \rightarrow Ax$ , where  $A$  is sparse matrix with condition  $\det A \neq 0$ . Map  $\tau F_{n,\alpha,\beta} \tau^{-1}$  written as a multivariate public rule:

$$x_1 \rightarrow h_1(x_1, x_2, \dots, x_n)$$

$$x_2 \rightarrow h_2(x_1, x_2, \dots, x_n)$$

...

$$x_n \rightarrow h_n(x_1, x_2, \dots, x_n),$$

can be used in public key cryptography. Alice - the holder of the key - keeps linear transformation and  $(\beta_1, \alpha_1, \beta_2, \alpha_2, \dots, \beta_k, \alpha_k)$  secret. Bob (public user) has the above map.

Combining the transformation  $F_{n,\alpha,\beta}$  with two linear transformation, Bob get a formula:

$$y = (h_1(x_1, \dots, x_n), \dots, h_n(x_1, \dots, x_n)),$$

where  $h_i(x_1, \dots, x_n)$  are polynomials of  $n$  variables of degree  $\lfloor \frac{n+2}{4} \rfloor$ . Hence the process of straightforward encryption can be done in polynomial time  $O(n^6)$ . But the cryptanalyst Catherine, having a only a formula for  $y$ , has very hard task to solve the system of  $n$  equations in  $n$  variables of degree  $\lfloor \frac{n+2}{4} \rfloor$ . So the general algorithm for finding the solution of system of polynomials equations has exponential time  $(\lambda n)^{O(n)}$ .

## 4.2 Diffie-Hellman key exchange protocol

We consider Diffie-Hellman algorithm for  $C(K^n)$  for the key exchange in the case of group. Let  $AGL_n(F_q)$  be the group of affine transformation of the vector space  $F_q^n$ , i.e. maps  $\tau_{A,b} : \tilde{x} \rightarrow \tilde{x}A + b$ , where  $\tilde{x} = (x_1, x_2, \dots, x_n)$ ,  $b = (b_1, b_2, \dots, b_n)$  and  $A$  is invertible sparse matrix with  $\det A \neq 0$ . Let  $h_n^k$  be the new public rule obtained via  $k$  iterations of  $h_n = F_{n,\alpha,\beta} = L_{D,n,\beta_1} P_{D,n,\alpha_1} L_{D,n,\beta_2} P_{D,n,\alpha_2} \dots L_{D,n,\beta_k} P_{D,n,\alpha_k}$ . Correspondents Alice and Bob have different information for making computation. Alice chooses dimension  $n$ , element  $h_n$  as above, affine transformation  $\tau \in AGL_n(K)$ . So she obtains the base  $b = \tau h_n^k \tau^{-1}$  and sends it in the form of standard polynomial map to Bob.

So Alice chooses rather large number  $n_A$  computes  $c_A = b^{n_A}$  and sends it to Bob. On his turn Bob chooses his own key  $n_B$  and computes  $c_B = b^{n_B}$ . He and Alice get the collision map  $c$  as  $c_A^{n_B}$  and  $c_B^{n_A}$  respectively.

Notice that the position of adversary is similar to Bob's position. He (or she) need to solve one of the equations  $b^x = c_B$  or  $b^x = c_A$ . The algorithm is implemented in the cases of finite fields and rings  $Z_m$  for family of groups  $C(K^n)$ .

## References

- [1] B. Bollobás, *Extremal Graph Theory*, Academic Press, London, 1978.
- [2] Jon-Lark Kim, U. N. Peled, I. Perepelitsa, V. Pless, S. Friedland, *Explicit construction of families of LDPC codes with no 4-cycles*, Information Theory, IEEE Transactions, 2004, v. 50, Issue 10, 2378 - 2388.
- [3] A. Lubotsky, R. Philips, P. Sarnak, *Ramanujan graphs*, J. Comb. Theory., 115, N 2., (1989), 62-89.
- [4] G. A. Margulis, *Explicit construction of graphs without short cycles and low density codes*, Combinatorica, 2, (1982), 71-78.
- [5] V. A. Ustimenko, *Graphs with Special Arcs and Cryptography*, Acta Applicandae Mathematicae, 2002, vol. 74, N2, 117-153.
- [6] V. A. Ustimenko, *Linguistic Dynamical Systems, Graphs of Large Girth and Cryptography*, Journal of Mathematical Sciences, Springer, vol.140, N3 (2007) pp. 412-434.
- [7] V. A. Ustimenko, *On the graph based cryptography and symbolic computations*, Serdica Journal of Computing, Proceedings of International Conference on Application of Computer Algebra, ACA-2006, Varna, N1 (2007).
- [8] V. A. Ustimenko, *Maximality of affine group, and hidden graph cryptosystems*, J. Algebra and Discrete Math., 10 (October 2004), 51-65.
- [9] V. A. Ustimenko, *CRYPTIM: Graphs as Tools for Symmetric Encryption*, in Lecture Notes in Computer Science, Springer, 2001, v. 2227, 278-287.
- [10] V. A. Ustimenko, A. Wrblewska, *Dynamical systems as the main instrument for the constructions of new quadratic families and their usage in cryptography*, Annales UMCS Informatica AI, ISSN 1732-1360.
- [11] A. Wrblewska *On some properties of graph based public keys*, Albanian Journal of Mathematics, Volume 2, Number 3, 2008, 229-234, NATO Advanced Studies Institute: "New challenges in digital communications".
- [12] E. H. Moore, *Tactical Memoranda*, Amer. J. Math., v.18, 1886, 264-303.
- [13] F. Lazebnik, V. A. Ustimenko, A. J. Woldar, *A Characterization of the Components of the graphs  $D(k, q)$* , Discrete Mathematics, 157 (1996) 271-283.
- [14] F. Lazebnik F. and V. Ustimenko, *Explicit construction of graphs with an arbitrary large girth and of large size*, Discrete Appl. Math. , 60, (1995), 275 - 284.
- [15] N.L. Biggs, *Graphs with large girth*, Ars Combinatoria, 25C (1988), 73-80.





---

# Session 5: Nonstandard Applications of Computer Algebra

---

Organizers:

Francisco Botana  
Antonio Hernando  
Eugenio Roanes-Lozano  
Michael Wester



# Similarity Detection for Rational Curves

Juan G. Alcázar, Carlos Hermoso  
Universidad de Alcalá (Spain)

Georg Muntingh  
University of Oslo (Norway)

`juange.alcazar@uah.es`

## Abstract

In Pattern Recognition, there is a vast literature concerning the question how to detect whether two curves are *similar*. Essentially, the problem is to recognize a certain curve as the result of applying a movement to another curve in a database. Most of the strategies proposed so far deal with curves in implicit form, and ultimately resort to numerics to decide whether such curves are related by a similarity.

In this talk, we present a new, fast, and deterministic algorithm to address the problem in the case when the curves are defined by a rational parametrization in exact arithmetic. The algorithm does not require to compute or use implicit equations of the curves, and takes advantage of the fact that the curves are similar if and only if their parametrizations are related by means of a Möbius transformation. It has been implemented and tested in the **Sage** computer algebra system, and shows good performance for middle inputs.

## Keywords

Pattern Recognition, Planar Rational Curves, Möbius transformation

# Envelope computation in dynamic geometry systems

Francisco Botana  
Universidad de Vigo (Spain)

Tomas Recio  
Universidad de Cantabria (Spain)

`fbotana@uvigo.es`

## Abstract

Considerable attention has been given to the computation of geometric loci in dynamic geometry, from both graphical and equational viewpoints. Recent work has established a rigorous approach to the last issue, solving the subject for the algebraic realm. Nevertheless, although the automatic computation of envelopes could be seen as an analogous problem, there are cases where unexpected difficulties emerge.

In this talk we review the state of the art of common dynamic geometry software when dealing with envelopes. Despite their maturity in other subjects, envelopes are generally considered as purely graphic objects in such environments, without any analytic knowledge about them.

We also describe a data structure needed to cope with envelopes in dynamic geometry, and a Sage program able to compute usual envelopes in an efficient way. Finally, in order to show the complexities of such computations, we discuss the envelope of a simple family of ellipses. The search for such envelope will illustrate two facts:

1. There is no general agreement between dynamic geometry developers about the definition of envelope, and
2. Currently, the simple application of computer algebra techniques is not enough to automatically solve the problem.

## Keywords

Dynamic Geometry, Automated Deduction in Geometry, Envelope Computation

## 1 Introduction

Given a family of curves  $C_\alpha : F(x, y, \alpha) = 0$ , its *envelope* or *discriminant* is defined [1] as the set

$$\mathcal{D} = \{(x, y) \in \mathbb{R}^2 : \text{there exists } \alpha \in \mathbb{R} \text{ with } F(x, y, \alpha) = \frac{\partial F}{\partial \alpha} = 0\}.$$

Other definitions coexist with this one, for instance

- The envelope  $E_1$  is the limit of intersections of nearby curves  $C_\alpha$ .
- The envelope  $E_2$  is a curve tangent to the  $C_\alpha$ .
- The envelope  $E_3$  is the boundary of the region filled by the curves  $C_\alpha$ .

where it can be proved that  $E_i \subset \mathcal{D}, i = 1, \dots, 3$ . While  $E_1$  seems to be the interpretation of envelopes given by Lagrange to singular solutions of differential equations (see [2]),  $E_3$  and, to a lesser extent,  $E_2$  are behind the intuitive notion of envelope used in dynamic geometry environments. Since these systems are mostly based on a graphical simulation of geometry, their ability to trace geometric elements is successfully used to suggest envelopes. Consider, for instance, the family of ellipses with foci in  $A(4, 0)$ ,  $B(0, \alpha)$  (a semifree point on the  $y$  axis) and major axis with length 5.

If a user activates the trace option for the variable ellipse and moves the point  $B$  along its path, a plane region is drawn (Figure 1), the border being the sought envelope, if the third alternative

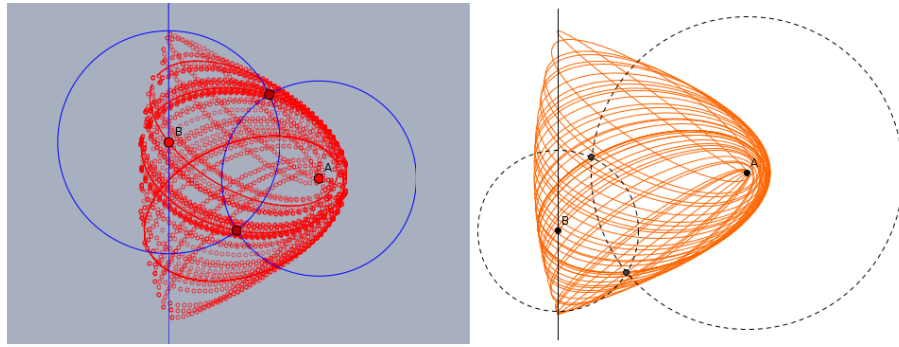


Figure 1: A family of ellipses obtained as loci (left: Cinderella, right: GeoGebra) is traced to suggest its envelope.

definition is used. Nevertheless, as usual in dynamic geometry, the user gets a cursory knowledge: no result about the type of curves defining the border is returned. Even worse, consider a region with holes, or without border. In this last case, the strategy of tracing the family curves could mislead an inexperienced user, as exemplified by searching for the envelope of straight lines passing through the origin.

It should be noted that although there exist a well known dynamic geometry software, Cabri, able to compute equations for constructed objects, its numerical approach is not robust and does not return any result for the above family.

## 2 A parametric approach for the envelope problem

Several authors (see, for instance, [3, 4]) have proposed extending the data structure of dynamic geometry systems to include what can be called a *parametric description* of constructions. This description involves keeping the relation between primitive and dependent objects in such a way that any assignment of the free variables (i.e., coordinates of basic points and equations of other initial objects) would trigger the *actual* computation of dependent objects.

Using the Sage library in [5], a generic ellipse of the family could be defined by

```
FreePoint('A',4,0)
FreePoint('P1',0,0)
FreePoint('P2',0,1)
Line('y','P1','P2')
PointOnObject('B','y')
FreePoint('M',2,2)
FreePoint('N',2,7)
Line('MN','M','N')
PointOnObject('P','MN')
Circle('c1','A','M','P')
Circle('c2','B','N','P')
IntersectionObjectObject('X','c1','c2')
Locus2('loc','X','B','P')
```

where the `Locus2` function contains a parametric representation of the ellipse. That is, its algebraic description is not a function in two variables, but it also contains the parameter of the variable point  $B$ . The polynomial of the family is

$$4y^2\alpha^2 - 4y\alpha^3 - 36x^2 - 100y^2 + \alpha^4 - 32xy\alpha + 16x\alpha^2 + 164y\alpha - 82\alpha^2 + 144x + 81,$$

and one could then use the first definition of envelope to find its equation. The elimination of  $\alpha$  returns

$$x^2y^4 + y^6 - 16x^3y^2 - 24xy^4 - 36x^4 + 74x^2y^2 - 2y^4 + 432x^3 + 32xy^2 - 1647x^2 - 207y^2 + 1656x + 1296,$$

and, after factoring,

$$(y^2 - 18x - 9)(y^2 + 2x - 9)(x^2 + y^2 - 8x + 16).$$

Thus, the border of the family of ellipses consists of (part) of the above parabolas. Nevertheless,...

### 3 Things are not so simple

There is a third factor in the expression of the discriminant that is not part of the border. In fact, this factor is the focus  $A$ ! While understanding why this point appears as part of the discriminant has not been a trivial task (as will be illustrated in the talk), we note that asking, for instance, Wolfram|Alpha, should give a hint about what is happening (Figure 2).

The screenshot shows the WolframAlpha interface with the following content:

**WolframAlpha** computational knowledge engine

Resolve[Exists[a, 4\*y^2\*a^2 - 4\*y\*a^3 - 36\*x^2 - 100\*y^2 + a^4 - 32\*x\*y\*a - ☆]

Input:

Resolve[  
 $\exists_a (4y^2a^2 - 4ya^3 - 36x^2 - 100y^2 + a^4 - 32xya + 16xa^2 + 164ya - 82a^2 + 144x + 81 = 0 \wedge 4a^3 - 12a^2y + 8ay^2 + 32xa - 32xy - 164a + 164y = 0)$   
 $e_1 \wedge e_2 \wedge \dots$  is the logical AND function »  
 $\exists_x$  expr represents the statement that there exists a value of  $x$  for which expr is True »

Result:

$18x - y^2 + 9 = 0 \vee 2x + y^2 - 9 = 0 \vee x^2 - 8x + y^2 + 16 = 0$   
 $e_1 \vee e_2 \vee \dots$  is the logical OR function »

Alternate forms:

$18x + 9 = y^2 \vee 2x + y^2 = 9 \vee (x - 4)^2 + y^2 = 0$   
 $18x + 9 = y^2 \vee 2x + y^2 = 9 \vee x^2 + y^2 + 16 = 8x$   
 $x = \frac{9}{2} - \frac{y^2}{2} \vee x = \frac{y^2}{18} - \frac{1}{2} \vee -iy = 4 - x \vee iy = 4 - x$

Figure 2: Wolfram|Alpha suggests that point  $A(4, 0)$  comes from complex components of the envelope.

The moral of this short note is the need of a most rigorous approach when applying algebraic methods valid in  $\mathbb{C}$  to misunderstood situations. Here, the family of ellipses is semialgebraic. Thus, automated approaches relying on complex approaches should be used with caution!

### Acknowledgement

The authors have been partially supported by the Spanish “Ministerio de Economía y Competitividad” and the “European Regional Development Fund” (FEDER), under the project MTM2011-25816-C02-02.

### References

- [1] J.W. Bruce, P.J. Giblin, *Curves and Singularities*. Cambridge: Cambridge University Press, 1984.
- [2] R.C. Yates, *A Handbook on Curves and Their Properties*. Ann Arbor, MI: J. W. Edwards, 1952.
- [3] F. Botana, On the Parametric Representation of Dynamic Geometry Constructions, in B. Murgante *et al.* (Eds.), *Computational Science and Its Applications – ICCSA 2011*, Springer LNCS 6785, pp. 342–352, 2011.

- [4] E. Roanes-Lozano, E. Roanes-Macías, M. Villar, A bridge between dynamic geometry and computer algebra. *Mathematical and Computer Modelling* 37, pp. 1005–1028, 2003.
- [5] Sage Automated Discovery library, <http://webs.uvigo.es/fbotana/AutDiscLib.txt>.

# Obtaining combinatorial structures associated with low-dimensional Leibniz algebras

Manuel Ceballos, Juan Núñez  
University of Seville (Spain)

Ángel F. Tenorio  
Pablo de Olavide University (Spain)

mceballos@us.es

## Abstract

In this paper, we analyze the relation between Leibniz algebras and combinatorial structures. More concretely, we study the properties to be satisfied by (pseudo)digraphs so that they are associated with low-dimensional Leibniz algebras. We present some results related to this association and show an algorithmic method to obtain them, which has been implemented with Maple.

## Keywords

Pseudodigraph, Combinatorial structure, Leibniz algebra, Structure Theory, Algorithm

## 1 Introduction

Leibniz algebras were introduced at the beginning of the 1990s by J.-L. Loday [3]. They are a particular case of non-associative algebras and provide a non-commutative generalization of Lie algebras. There exists extensive research on these algebras due to their many applications in Engineering, Physics and Applied Mathematics. However, some aspects of Leibniz algebras remain unknown. In fact, the classification of nilpotent and solvable algebras is still an open problem.

Graph Theory is also very important and useful due to its many uses as a tool for other subjects. Our main goal is to extend the study and analysis of the relations between Graph Theory and Lie algebras proposed in [1, 2], but this time to the case of Leibniz algebras.

## 2 Preliminaries

We show some preliminary concepts on Leibniz algebras, bearing in mind that the reader can consult [3] as an introductory paper.

**Definition 1** A Leibniz algebra  $\mathcal{L}$  over a field  $\mathbb{K}$  is a vector space with a second inner bilinear composition law  $[\cdot, \cdot]$ , which verifies the so-called Leibniz identity

$$[[X, Y], Z] - [[X, Z], Y] - [X, [Y, Z]] = 0, \quad \forall X, Y, Z \in \mathcal{L}$$

From now on, we will denote  $L(X, Y, Z) = [[X, Y], Z] - [[X, Z], Y] - [X, [Y, Z]]$ .

If, in addition, is verified that  $[X, X] = 0$ , for all  $X \in \mathcal{L}$ , the Leibniz algebra is also a Lie algebra. In this case, it is satisfied that  $[X, Y] = -[Y, X]$  and the Leibniz identity is equivalent to the Jacobi identity.

**Definition 2** Given a basis  $\{e_i\}_{i=1}^n$  of an  $n$ -dimensional Leibniz algebra  $\mathcal{L}$ , its structure constants are defined by  $[e_i, e_j] = \sum_{h=1}^n c_{i,j}^h e_h$ , for  $1 \leq i, j \leq n$ .

**Definition 3** The derived and central series of a finite-dimensional Leibniz algebra  $\mathcal{L}$  are

$$\mathcal{L}_1 = \mathcal{L}, \quad \mathcal{L}_2 = [\mathcal{L}, \mathcal{L}], \quad \dots, \quad \mathcal{L}_k = [\mathcal{L}_{k-1}, \mathcal{L}_{k-1}], \quad \dots \quad \text{and} \quad \mathcal{L}^1 = \mathcal{L}, \quad \mathcal{L}^2 = [\mathcal{L}, \mathcal{L}], \quad \dots, \quad \mathcal{L}^k = [\mathcal{L}^{k-1}, \mathcal{L}], \quad \dots$$

So,  $\mathcal{L}$  is called  $(m-1)$ -step solvable (resp. nilpotent) if there exists  $m \in \mathbb{N}$  such that  $\mathcal{L}_m = \{0\}$  and  $\mathcal{L}_{m-1} \neq \{0\}$  (resp.  $\mathcal{L}^m = \{0\}$  and  $\mathcal{L}^{m-1} \neq \{0\}$ ).



### 3 Associating combinatorial structures with Leibniz algebras

Let  $\mathcal{L}$  be a  $n$ -dimensional Leibniz algebra with basis  $\mathcal{B} = \{e_i\}_{i=1}^n$ . Its structure constants correspond to  $[e_i, e_j] = \sum_{h=1}^n c_{i,j}^h e_h$  and, hence, the pair  $(\mathcal{L}, \mathcal{B})$  is associated with a combinatorial structure by the following procedure

- a) For each  $e_i \in \mathcal{B}$ , we draw a vertex  $i$ .
- b) For every vertex  $i$  verifying  $[e_i, e_i] \neq 0$ , we draw a loop such that its weight is an  $n$ -tuple given by  $(c_{i,i}^1, c_{i,i}^2, \dots, c_{i,i}^n)$ .
- c) Given two vertices  $i, j$  verifying  $(c_{i,j}^j, c_{j,i}^j) \neq (0, 0)$ , we draw a directed edge from vertex  $i$  to  $j$  whose weight is given by the pair  $(c_{i,j}^j, c_{j,i}^j)$ .
- d) Given three vertices  $i < j < k$  such that  $(c_{i,j}^k, c_{j,i}^k, c_{j,k}^i, c_{k,j}^i, c_{i,k}^j, c_{k,i}^j) \neq (0, 0, 0, 0, 0, 0)$ , we draw a full triangle  $ijk$  such that the edges  $ij$ ,  $jk$  and  $ik$  have weights  $(c_{i,j}^k, c_{j,i}^k)$ ,  $(c_{j,k}^i, c_{k,j}^i)$  and  $(c_{i,k}^j, c_{k,i}^j)$ , respectively. Moreover,
  - d1) we use a discontinuous line (named *ghost edge*) for edges with weight  $(0, 0)$ .
  - d2) If two triangles  $ijk$  and  $ijl$  satisfy  $(c_{i,j}^k, c_{j,i}^k) = (c_{i,j}^l, c_{j,i}^l)$ , draw only one edge between vertices  $i$  and  $j$  shared by both triangles.

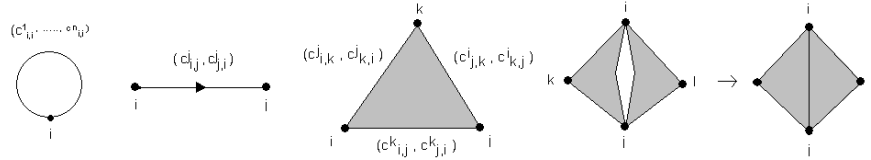


Figure 1: Loop, directed edge, full triangle and two triangles sharing an edge.

### 4 Leibniz algebras and (pseudo)digraphs

In this section, we study the structure of digraphs associated with low-dimensional Leibniz algebras. For each case, we will study the type of Leibniz algebra according to the solvability of this algebra. To be associated with a (pseudo)digraph  $G$ , a given Leibniz algebra  $\mathcal{L}$  with basis  $\mathcal{B} = \{e_i\}_{i=1}^n$  has the following law

$$[e_i, e_j] = c_{i,j}^i e_i + c_{i,j}^j e_j, \quad 1 \leq i \neq j \leq n; \quad [e_k, e_k] = \sum_{h=1}^n c_{k,k}^h e_h \quad (1)$$

since these brackets avoid the appearance of full triangles in  $G$ .

**Proposition 1** *Every digraph admitting some configuration of [1, Fig. 9] as a subdigraph is not associated with any Leibniz algebra.*

**Proposition 2** *The abelian Leibniz algebra is the only one of dimension 1, associated with a digraph.*

**Proposition 3** *Let  $\mathcal{L}$  be a 2-dimensional Leibniz algebra associated with a connected pseudodigraph  $G$ . Then, the configuration d) shown in Figure 2 is forbidden in  $G$ . In fact,  $G$  must present one of the remaining configurations in that figure. Moreover, it is verified that*

- Configurations a) and c) are associated with 2-step solvable non-nilpotent Leibniz algebras.

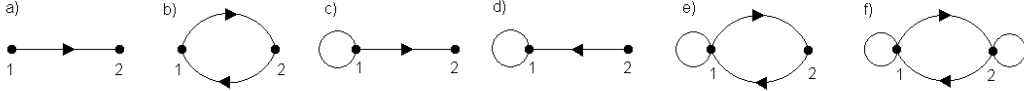


Figure 2: Pseudodigraphs with two vertices and associated with Leibniz algebras.

- Configuration b) is always associated with 2-step solvable non-nilpotent Lie algebras (i.e. only commutative Leibniz algebras).
- Configurations e) and f) are associated with a 2-step nilpotent Leibniz algebras.

**Example 1** Let  $\mathcal{L}$  be the Leibniz algebra with brackets  $[e_2, e_1] = e_2$  associated with Configuration a). In this case,  $\mathcal{L}_2 = \mathcal{L}^2 = \langle e_2 \rangle$ , whereas  $\mathcal{L}^i = \mathcal{L}_2$  and  $\mathcal{L}_i = 0$ , for all  $i \geq 3$ . Therefore,  $\mathcal{L}$  is 2-step solvable, non-nilpotent.

**Example 2** We consider the Leibniz algebra  $\mathcal{L}$  with law  $[e_1, e_1] = -e_1 - e_2$ ,  $[e_1, e_2] = e_1 + e_2$  associated with Configuration e). In this case,  $\mathcal{L}^2 = \mathcal{L}_2 = \langle e_1 + e_2 \rangle$  and  $\mathcal{L}_3 = \mathcal{L}^3 = 0$ . Hence,  $\mathcal{L}$  is 2-step nilpotent.

**Example 3** Let  $\mathcal{L}$  be the Leibniz algebra with brackets  $[e_1, e_1] = [e_2, e_2] = -e_1 - e_2$ ,  $[e_1, e_2] = [e_2, e_1] = e_1 + e_2$ , associated with Configuration f). For this algebra,  $\mathcal{L}_2 = \langle e_1 + e_2 \rangle$ ,  $\mathcal{L}_3 = \mathcal{L}^3 = \{0\}$ . So,  $\mathcal{L}$  is 2-step nilpotent.

**Proposition 4** Let  $\mathcal{L}$  be a 3-dimensional Leibniz algebra associated with a connected pseudograph  $G$  including some loop. Then,  $G$  must present one of the configurations in Figure 3 up to permutation of labels. Any other pseudodigraph is forbidden in  $G$ .

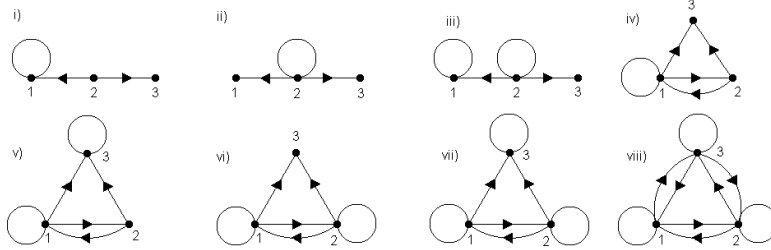


Figure 3: Pseudodigraphs with three vertices, associated with Leibniz algebras, not being Lie algebras.

**Proposition 5** Let  $G$  be a pseudodigraph formed by the first configuration of [1, Fig. 15] with loops. Then  $G$  is associated with a solvable non-nilpotent Leibniz algebra.

**Proposition 6** Let  $G$  be a pseudodigraph formed by the second configuration of [1, Fig. 15] with loops. Then,  $G$  is associated with a Leibniz algebra if and only if  $G$  has a loop on each vertex incident with a double edge.

## 5 Implementation and complexity for the Leibniz identity

Now, we show the algorithmic method that we have used in the previous section to evaluate the Leibniz identity in order to find out the allowed and forbidden configurations and the restrictions over the weights of the edges. Regarding this, we have implemented our algorithm using the symbolic computation package MAPLE, working the implementation in version 12 or higher. To do this, we will use the libraries `linalg`, `combinat`, `GraphTheory` and `Maplets[Elements]` to activate commands related to Linear and Combinatorial Algebra, Graph Theory and the last one to display a message so that the user introduces the required input in the first subprocedure. So, we start considering a vector space  $\mathcal{L}$  with basis  $\mathcal{B}$  and the type of brackets expressed in (1) and give the following steps:

1. Computing the bracket product between two arbitrary basis vectors in  $\mathcal{B}$ .

This first subprocedure is called `law` and computes the bracket between two arbitrary basis vectors in  $\mathcal{B}$ . It receives the subindexes of two basis vectors in  $\mathcal{B}$ . A conditional sentence is introduced to determine each non-zero bracket. The user has to complete the implementation depending on the law of  $\mathcal{L}$ , so we have added a sentence at the beginning of the implementation, reminding of this fact. Before running any other sentence, we restart all the variables by using the command `restart`. Moreover, we save the value of variable `dim` (the dimension) with the command `assign`.

```
> maplet:=Maplet(AlertDialog("Don't forget to introduce non-zero brackets and the dimension in
subprocedure law", 'onapprove'=Shutdown("Continue"), 'oncancel'=Shutdown("Aborted"))):
> Maplets[Display](maplet):
> assign(dim,...):
> law:=proc(i,j)
>   if (i,j)=... then ...;
>   elif ....
>   else 0; end if;
> end proc;
```

2. Evaluating the bracket between two vectors expressed as a linear combination of vectors from basis  $\mathcal{B}$ .

We implement the subprocedure called `bracket` to compute the product between two arbitrary vectors of  $\mathcal{L}$ , which are expressed as linear combinations of the vectors in  $\mathcal{B}$ . The subprocedure `law` is called in the implementation.

```
> bracket:=proc(u,v,n)
>   local exp; exp:=0;
>   for i from 1 to n do
>     for j from 1 to n do
>       exp:=exp + coeff(u,e[i])*coeff(v,e[j])*law(i,j);
>     end do;
>   end do;
>   exp;
> end proc;
```

3. Imposing the Leibniz identity and solving the corresponding system of equations.

Next, we show the implementation of the main procedure called `Leibniz`, which checks if the vector space  $\mathcal{L}$  is or not a Leibniz algebra. This procedure receives as input the dimension  $n$  of the vector space  $\mathcal{L}$  and returns the solution of a system of equations obtained from imposing the Leibniz identity in  $\mathcal{L}$ . If the system has no solution, then we can conclude that the vector space  $\mathcal{L}$  is not a Leibniz algebra. Otherwise, we will obtain the conditions over the structure constants  $c_{i,j}^k$  so that  $\mathcal{L}$  is a Leibniz algebra.

```
> Leibniz:=proc(n)
>   local L,M,N,P;
>   L:=[];M:=[];N:=[];P:=[];
>   for i from 1 to n do
>     L:=[op(L),i,i,i];
>   end do;
>   M:=permute(L,3);
>   for j from 1 to nops(M) do
>     eq[j]:=bracket(bracket(e[M[j][1]],e[M[j][2]],n),e[M[j][3]],n)-
>       bracket(bracket(e[M[j][1]],e[M[j][3]],n),e[M[j][2]],n)-
>       bracket(e[M[j][1]],bracket(e[M[j][2]],e[M[j][3]],n),n);
>   end do;
>   N:=[seq(eq[k], k=1..nops(M))];
>   for k from 1 to nops(N) do
>     for h from 1 to n do
>       P:=[op(P),coeff(N[k],e[h])=0];
>     end do;
>   end do;
>   solve(P);
> end proc;
```

**Example 4** Now, we show an example with the configuration  $i$ ) from Figure 3. We consider the 3-dimensional vector space  $\mathcal{L}$  with brackets

$$[e_1, e_1] = \sum_{i=1}^3 c_{1,1}^i e_i; [e_j, e_2] = c_{j,2}^j e_j, [e_2, e_j] = c_{2,j}^j e_j, \text{ for } j = 1, 3$$

First, we have to complete the implementation of the subprocedure `law` as follows

```
> maplet:=Maplet(AlertDialog("Don't forget to introduce non-zero brackets and the dimension in
subprocedure law", 'onapprove'=Shutdown("Continue"), 'oncancel'=Shutdown("Aborted"))):
> Maplets[Display](maplet):
> assign(dim,3):
> law:=proc(i,j)
>   if (i,j)=(1,1) then c111*e[1]+c112*e[2]+c113*e[3];
>   elif (i,j)=(1,2) then c121*e[1];
>   elif (i,j)=(2,1) then c211*e[1];
>   elif (i,j)=(2,3) then c233*e[3];
>   elif (i,j)=(3,2) then c323*e[3];
>   else 0;
> end if;
> end proc;
```

After that, we must run the subprocedure `bracket` and the procedure `Leibniz`. Now, we evaluate this main procedure over the variable `dim`

```
> Leibniz(dim);
> {c111=0,c112=0,c113=c113,c121=-c211,c211=c211,c233=0,c323=-2*c211}
```

So, we obtain those restrictions for the weights of the edges in configuration  $i$ ) from Figure 3.

Next, we compute the complexity of the algorithm. To do so, we consider the number of operations carried out in the worst case. We use the big  $O$  notation to express the complexity. To recall the big  $O$  notation, the reader can consult [4]: given two functions  $f, g : \mathbb{R} \rightarrow \mathbb{R}$ , we could say that  $f(x) = O(g(x))$  if and only if there exist  $M \in \mathbb{R}^+$  and  $x_0 \in \mathbb{R}$  such that  $|f(x)| < M \cdot |g(x)|$ , for all  $x > x_0$ .

We denote by  $N_i(n)$  the number of operations when considering the step  $i$ . This function depends on the dimension  $n$  of the Lie algebra. Table 1 shows the number of computations and the complexity of each step, as well as indicating the name of the procedure corresponding to each step.

Table 1: Complexity and number of operations.

Step	Procedure	Complexity	Operations
1	<code>law</code>	$O(n^2)$	$N_1(n) = O\left(\frac{n(n-1)}{2}\right)$
2	<code>bracket</code>	$O(n^4)$	$N_2(n) = \sum_{i=1}^n \sum_{j=1}^n N_1(n)$
3	<code>Leibniz</code>	$O(n^7)$	$N_3(n) = O(n) + O(n^3) + \sum_{i=1}^{n^3} N_2(n) + \sum_{j=1}^{n^3} \sum_{k=1}^n 1$

## References

- [1] A. Carriazo, L.M. Fernández, J. Núñez, Combinatorial structures associated with Lie algebras of finite dimension, *Linear Algebra Appl.* 389 (2004), 43–61.
- [2] J. Cáceres, M. Ceballos, J. Núñez, M.L. Puertas, A.F. Tenorio, Combinatorial structures of three vertices and Lie algebras, *Int. J. Computer Math.* 89:13–14 (2012), 1879–1900.
- [3] J.L. Loday, Une version non commutative des algèbres de Lie: les algèbres de Leibniz, *Enseign. Math.* (2), 39 (1993), pp. 269–293.
- [4] H.S. Wilf, *Algorithms and Complexity*, Prentice Hall, Englewood Cliffs, 1986.

# Designing Hamiltonian Cycles

Francisco de Arriba, Eusebio Corbacho, Ricardo Vidal  
University of Vigo (Spain)

`corbacho@uvigo.es`

## Abstract

Historically, the minimal length Hamiltonian cycles in a random point cloud lying inside a given rectangle are computed by partitioning this rectangle. We have used successive convex hulls of the set of points, in order to obtain partitions better suited for this purpose. The free computer algebra system Sage has been very useful to perform the corresponding computations (for sets of 100 to 200 points, the result is obtained in just 15 seconds using a laptop computer running Ubuntu 12.04 with an Intel Core i7-2630QM processor and 8GB of RAM).

The code developed is also applied with success to obtain good approximations of minimal length Hamiltonian cycles, across the major cities of the countries of the European Union. In each country,  $E_i$ , we make a transverse Mercator representation centered in the point  $C_i$  of average latitude and average longitude among the selected cities in the country. For a list of countries  $[E_1, \dots, E_n]$  we paste in the origin of the complex plane the local chart of  $E_1$ . Then, the local chart of  $E_2$  is translated by the complex number whose modulus is the geodesic distance  $(C_1, C_2)$  and whose argument is the angle between the maximal circle  $(C_1, C_2)$  and the parallel of  $C_1$ , and so successively until  $E_n$ . In this way, all the cities are transformed into a set of points in the complex plane where each pair can be connected by a straight line.

## Keywords

Hamiltonian Cycle, Convex Hull, Jarvis algorithm modified, Sage, Geographic Coordinates, Geodesic Displacement

# 1 Introduction

The search of minimal length paths which pass just once through each one of the points of a finite subset of the complex plane,  $L$ , is a classical problem not yet solved in a reasonable computation time, when the cardinal  $|L|$  is big.

If  $R$  is a bounded rectangle containing  $L$ , good approximations to the optimal solution have been achieved using rectangular partitions  $\{R_i \mid i \in I\}$  of  $R$  which induce partitions  $\{L_i \mid i \in I\}$  in  $L$  so that  $L_i = L \cap R_i$  and  $|L_i| < k \quad \forall i \in I$  with  $k$  a small natural number. In these subsets  $L_i$  you can easily find minimal length hamiltonian paths and the standard computations are guided by different strategies to adequately connect the optimal paths for each  $L_i$  and generate the desired optimal hamiltonian cycle in all  $L$  [1].

In this communication we present a non-standard attempt of construction of the optimal hamiltonian cycle in any finite set  $L$  of the complex plane, based on the following ideas:

1. If  $co(L)$  is the convex envelope of  $L$ ,  $\partial(co(L))$  is its border and  $L \subset \partial(co(L))$  we should just choose an orientation in that border and, according to it, order the points of  $L$ . In this way we construct a closed hamiltonian path in  $L$  which will be of minimal length because it is the only one without crossing of edges.
2. If there exists a  $z_0 \in L$  such that  $L' = L \setminus \{z_0\}$  has the property expressed in 1, we can construct an optimal hamiltonian path in  $L'$  and replace the most suitable edge  $(z_i, z_{i+1})$  by the polygonal path  $(z_i, z_0, z_{i+1})$  so that the new path, which obviously would still be hamiltonian, enlarged its length as little as possible.
3. If there existed a  $\{z_0, \dots, z_n\} \subset L$  such that  $L' = L \setminus \{z_0, \dots, z_n\}$  had the property expressed in 1, we could consider the optimal hamiltonian path in  $L'$  and study the order to incorporate the  $z_i$  to the path  $L'$  to preserve the hamiltonian character and to enlarge its length as little as possible.

In any  $L$  we can find the subset  $L_1 = L \cap \partial(co(L))$  which obviously has the property expressed in 1. We add the elements of  $L \setminus L_1$  following the heuristic in 3, in order to find the optimal hamiltonian cycle of  $L_1$ . The elements of  $L_2 = L \cap \partial(co(L \setminus L_1))$  are added in such a way that provide the best Hamiltonian cycle in  $L_{12} = L_1 \cup L_2$ . We add the elements of  $L_3 = L \cap \partial(co(L \setminus L_{12}))$  and, so on. A Sage implementation of these ideas can be seen in [2].

In section 2 we describe some of these algorithms and discuss some examples of use in order to highlight their good computing times in an average laptop. In section 3 we present a simulation of optimal touristic or transport circuits through cities of the European Union so that the results can be compared with those offered in Internet by known sources of geographical information.

## 2 Hamiltonian Cycles

The function *listacomplejos*( $R, n$ ) returns a random list of  $n$  complex numbers contained in the central square of side  $2R$  which will be our working set  $L$ . The function *envolturaconvexa*( $L$ ) returns the set  $L_1 = L \cap \partial(co(L))$  counterclockwise ordered and the function *cebolla*( $L$ ) returns the list  $[L_1, L_2, \dots, L_n]$  expressing the desired partition of  $L$ .

The function *pegalistas*( $L_1, L_2$ ) returns the set  $L_{12}$  as an ordered list which tries to be the best possible hamiltonian cycle in the two first layers. The order of incorporation of the points of  $L_2$  to  $L_1$  is decided by the minimal length enlargement of the path. Ties are solved by the maximal incorporation angle and, if they persist, we use a recursive algorithm. Once decided the incorporation of a certain  $w \in L_2$  between the points  $(z_i, z_{i+1})$  of  $L_1$  one replaces the piece  $[z_{i-1}, z_i, w, z_{i+1}, z_{i+2}]$  by their optimal reordering and proceeds to incorporate a new element of  $L_2$ .

The function *cicloham*( $L$ ) obtains the list  $[L_1, L_2, \dots, L_n]$ , computes  $L_{12}$  pasting  $L_2$  to  $L_1$ ,  $L_{123}$  pasting  $L_3$  to  $L_{12}$  and, by iteration, proposes as optimal hamiltonian cycle in  $L$  the list  $L_{1\dots n}$ .

Our trust in this technique grew by its good work even in cases whose geometry did not suggest it. For example, if  $E$  is the set

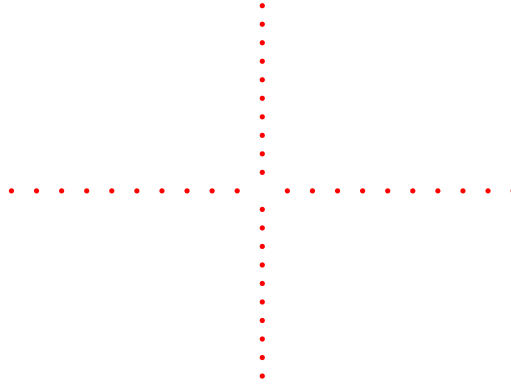


Figure 1: The set E

the hamiltonian cycle  $Q = cicloham(E)$  is

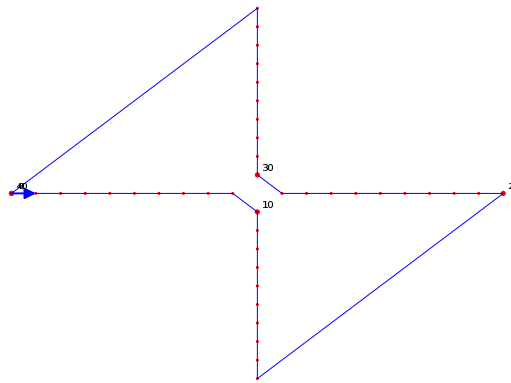


Figure 2: The cycle Q found in set E

which, evidently, is the optimal one.

However, in spite of being cautious in the process of pasting, the list  $L_{1...n}$  which always is a hamiltonian cycle, can present some crossings of edges and, so, not be the minimal length one. For example, if  $L$  is a set with  $|L| = 400$  in a 40 m length sided square,

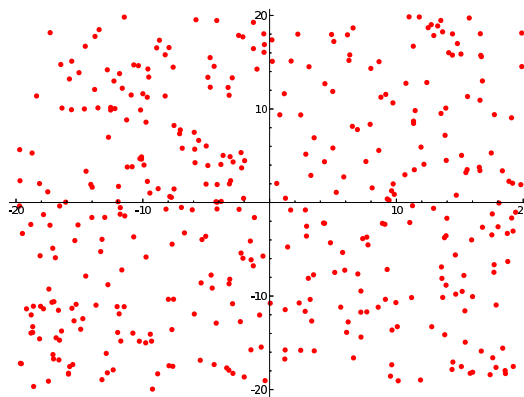


Figure 3: A set L of 400 cities

$C=cicloham(L)$  is a Hamiltonian cycle with a 654.54 m length which presents two crossings :

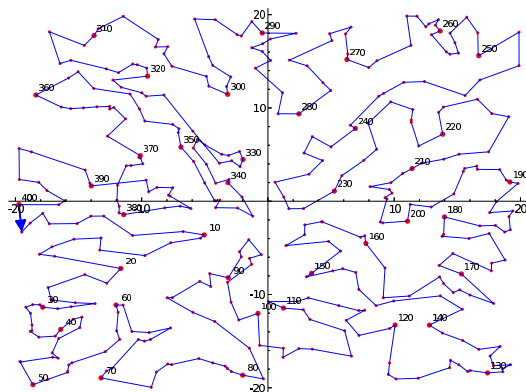


Figure 4: The cycle C found in L

However we can paste again the piece  $C[325 : 335]$  to the cycle  $C[: 325] + C[335 :]$  by means of the formula  $MC=mejoratramo(C,325,335)$  and the piece  $MC[370 : 390]$  to the cycle  $MC[: 370] + MC[390 :]$  and obtain a cycle  $OC=mejoratramo(MC,370,390)$  without crossings of 648.92 m.

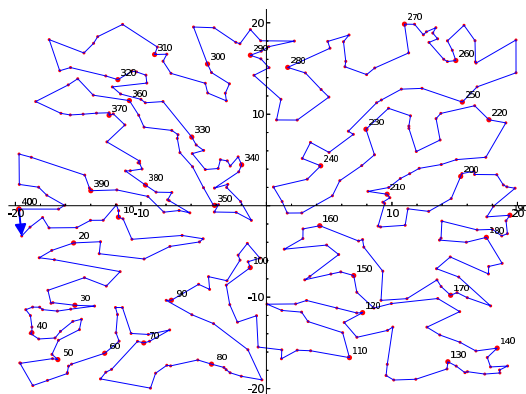


Figure 5: The cycle OC in L without crossings

Despite this technique does not assure finding the shortest hamiltonian path, its iteration gives a fair approximation if a suitable collaboration man-machine is established. Although the quantification of the goodness of this approximation is currently ongoing work, the heuristics makes us sure that our technique can be used in games of the type [3] without the limitation  $|L| \leq 50$ .

### 3 Hamiltonian trips

One of the more used applications of this type of problems is the design of touristic tours or routes of transport across a certain set of cities. In our case, we have tried to get that the representation of the cities in the complex plane can be realized simply from their latitude and longitude, to make it easy to the user to incorporate cities or places of his interest to the set of the 518 cities of the European Union considered by us.

In each country of the EU we have chosen one city per each million of inhabitants, and for that reason we have left Cyprus and Malta out. In the country  $E_i$ , we make a transverse Mercator representation centered in the point  $C_i$  of average latitude and average longitude among the selected cities in the country. For a list of countries  $[E_1, \dots, E_n]$  we paste in the origin of the complex plane the local chart of  $E_1$ . The local chart of  $E_2$  is then translated by the complex number whose modulus is the geodesic distance  $(C_1, C_2)$  and whose argument is the angle between the maximal circle  $(C_1, C_2)$  and the parallel of  $C_1$ , and so successively until  $E_n$ . This is realized by the function



$viaje([E_1, \dots, E_n])$  which uses, as auxiliary function, the function  $desplazamiento(E_i, E_{i+1})$ . The cartographical representation of the cities so obtained is also not standard and we have designed it to make it easy to the user the incorporation of new groups of cities. We think that the small distortions introduced by this representation should not affect the searched optimal hamiltonian cycle although eventually they can modify its real length. For example, the best Hamiltonian cycle across the cities of Spain and Portugal which we obtain with  $viaje([espanha, portugal])$  and a iterated use of the function  $mejoratramo$  is

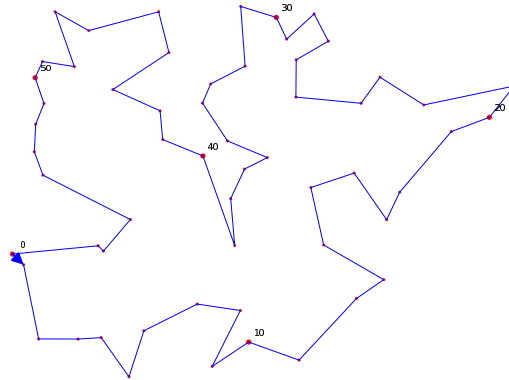


Figure 6: The cycle Spain and Portugal

- 0 [LISBOA, Setubal, Portimao, Tavira, Huelva, Cadiz, Sevilla, Cordoba, Jaen, Malaga]
- 10 [Granada, Almeria, Murcia, Alicante, Albacete, Cuenca, Teruel, Valencia, Castellon, Tarragona]
- 20 [Barcelona, Gerona, Lerida, Huesca, Zaragoza, Soria, Logronho, Pamplona, S. Sebastian, Vitoria]
- 30 [Bilbao, Santander, Burgos, Palencia, Valladolid, Segovia, Guadalajara, MADRID, Toledo, Ciudad Real]
- 40 [Avila, Salamanca, Zamora, Bragansa, Leon, Oviedo, Lugo, Corunha, Orense, Pontevedra]
- 50 [Valensa, Braga, Porto, Aveiro, Coimbra, Caceres, Badajoz, Elvas, LISBOA]

with a 5502.95 km length and the cities sequenced by groups of ten, to easily localize them in the graphic. Undoubtedly it seems to us more trustful the sequencing of the cycle than its length. This would be a minor question because in our planning we have taken into account neither the orography nor the road net. However, the number of cities seems to be enough to suppose that for each edge of the cycle there exists a road of the net which connects the two cities at its endpoints.

## References

- [1] Har-Peled, S. ; *Geometric Approximation Algorithms*, AMS Mathematical Surveys and Monographs Vol 173, (2011).
- [2] Arriba, F. Corbacho, E. Vidal, R. <https://dl.dropboxusercontent.com/u/21326323/ACA2013.sws>
- [3] TSP Games (<http://www.tsp.gatech.edu/games/index.html>)

# Designing rotating schedules by using Gröbner bases

Raúl Falcón<sup>1</sup>, David Canca<sup>1</sup>, Eva Barrena<sup>2</sup>

<sup>1</sup> University of Seville (Spain)

<sup>2</sup> CIRRELT and HEC Montréal (Canada)

{rafalgan, dco}@us.es, eva.barrena-algara@hec.ca

## Abstract

In the current paper, we deal with the problem of designing rotating schedules from an algebraic computational approach. Specifically, we determine a set of Boolean polynomials whose zeros can be uniquely identified with the set of rotating schedules related to a given workload matrix and with the different constraints which are usually imposed to them. These polynomials constitute zero-dimensional radical ideals, whose reduced Gröbner bases can be computed to determine explicitly the set of rotating schedules which satisfy each constraint and hence, making possible to analyze their influence in the final pattern. Finally, we use this polynomial method to classify and characterize the set of rotating schedules related to a given number of shifts and work teams.

## Keywords

Rotating schedule, Boolean ideal, Gröbner basis.

## 1 Introduction

Crew rostering is the last relevant step within the tactical phase of railway planning. Once the distinct shifts are designed to cover all programmed services, it becomes necessary to proceed with the individual assignment of the personnel. The high complexity of this last task is mainly due to the differences which exist among shifts (compare the most common: day, evening and night shifts) from a quantitative as well as from a qualitative point of view. In addition, the individual acquired rights of the personnel have to be taken into consideration. Shift works have special relevance in those facilities which provide a service which is available at any time and day of the week. Due to the mentioned significant differences among shifts, labor schedules in these jobs have to be carefully designed. A scheduling pattern which is highly recommended for shift works is that of rotating schedules, where the assignment of shifts per week to  $n$  distinct work teams is explicitly exposed in a schedule of  $n$  rows and 7 columns. Specifically, the  $(i, j)$  entry of the schedule corresponds to the shift or rest period which is initially assigned to the  $i^{\text{th}}$  team, the  $j^{\text{th}}$  day of the first week. Once the week finishes, each team moves down to the following row of the schedule (or to the first row in case of being the last team) to know the shift assignment of the new week.

In order to design a rotating schedule, it is necessary to know in advance its related *workload matrix*, that is, the number of shifts of each type which have to be assigned each day of the week. Besides, several constraints have to be taken into account to preserve equal opportunities among workers and to prevent health risks like stress, sleep disorder or digestive upsets. In the current paper, we consider the following six constraints exposed by Laporte [8, 9]:

- C.1) Schedules should contain as many full weekends off as possible.
- C.2) Weekends off should be well spaced out in the cycle.
- C.3) A shift change can only occur after at least one day off.
- C.4) The number of consecutive work days must not exceed 6 days and must not be less than 2.
- C.5) The number of consecutive rest days must not exceed 6 days and must not be less than 2.
- C.6) In consecutive days, forward rotations (day, evening, night) are generally preferred to backward rotations (day, night, evening).

There exist distinct methods and techniques in the literature to design rotating schedules [1] like manual approach, integer programming, heuristic procedures or network flows. Since the main goal of designing rotating schedules is minimizing costs and maximizing employee satisfaction, these methods do not determine in general all the possible rotating schedules verifying certain conditions, but only those which are on the path of finding the optimal model. However, it would be interesting to analyze the influence of each kind of constraint on the set of feasible solutions, that is, to deal with the number of rotating schedules which are eliminated or incorporated every time that we add or remove a specific condition. As a possible alternative, the combinatorial structure of any rotating schedule facilitates the use of the polynomial method established by Alon [2] and Bernasconi et al. [4], which solves enumeration and counting problems in Combinatorics by computing the reduced Gröbner basis of a zero-dimensional ideal uniquely related to a given combinatorial object. In this regard, see, for instance, the surveys of De Loera et al. [10, 11] on possible applications in graph theory. Indeed, graph theory has already been used in the scheduling problem [7].

The current paper is organized as follows. In Section 2, we identify the rotating schedules of a given workload matrix and satisfying Constraints C.1-C.6, with the set of zeros of a Boolean ideal, which can be explicitly determined by computing the corresponding reduced Gröbner basis. Such a computation has been implemented in a procedure in SINGULAR [6], which is used in Section 3 to study the influence of Constraints C.3-C.6 in the design of rotating schedules related to part time employers. Finally, since Gröbner bases are extremely sensitive to the number of variables, we show in Section 4 how the previous method can be improved by considering column generation.

## 2 Boolean polynomials related to rotating schedules.

Given two positive integers  $s, t \in \mathbb{N}$ , let  $W = (w_{ij})$  be a  $s \times 7$  array with all column sums equal to  $t$  and let  $\text{RS}_W$  denote the set of rotating schedules of  $s$  shift works (including that corresponding to rest days) and  $t$  team works, which have  $W$  as workload matrix. That is,  $w_{ij}$  indicates the number of team works which have to have the  $i^{\text{th}}$  shift the  $j^{\text{th}}$  day. Thus, for instance, Constraint C.1 implies that any rotating schedule of  $\text{RS}_W$  should have  $f_W = \min\{w_{s6}, w_{s7}\}$  full weekends off.

Hereafter,  $[s] = \{1, \dots, s\}$  is assumed to represent the set of shift works of  $\text{RS}_W$  in forward rotation order (thus, for instance, 1, 2 and 3 can represent, respectively, day, evening and night shifts), where the last symbol  $s$  corresponds to a rest day. In particular, the set  $\text{RS}_W$  can be identified with that of  $t \times 7$  arrays  $R = (r_{ij})$  based on  $[s]$  such that the frequency vector of the symbols which appear in each column of  $R$  is given by the corresponding column of  $W$ , that is, given  $i \in [s]$  and  $j \in [7]$ , the  $j^{\text{th}}$  column of  $R$  contains  $w_{ij}$  times the symbol  $i$ .

In practice, it is also interesting to have the possibility of imposing some of the entries of our future rotating schedule. Thus, for instance, according to Constraint C.2, the symbols  $s$  corresponding to the  $f_W$  full weekends off could be distributed by hand in advance, in a well-spaced way in the cycle. Indeed, it is the usual way to proceed for designing rotating schedules [9]. In this regard, let  $E = (e_{ij})$  be a  $t \times 7$  array with entries in the set  $[s] \cup \{0\}$ , where  $e_{ij} \in [s]$  if the entry  $(i, j)$  is imposed to our rotating schedule, or zero, otherwise. We say that  $R = (r_{ij}) \in \text{RS}_W$  contains  $E$  if  $r_{ij} = e_{ij}$ , for all  $i \in [t]$  and  $j \in [7]$ . Let  $\text{RS}_{W,E}$  denote the subset of rotating schedules of  $\text{RS}_W$  containing  $E$ . The next result shows how this set can be identified with that of zeros of a Boolean ideal which is zero-dimensional and radical. Its reduced Gröbner basis can be then computed to determine explicitly the cardinality of  $\text{RS}_{W,E}$ .

**Theorem 1** *The set  $\text{RS}_{W,E}$  can be identified with that of zeros of the following zero-dimensional ideal of  $\mathbb{Q}[x_{111}, \dots, x_{t7s}]$ .*

$$\begin{aligned} I_{W,E} = & \langle 1 - x_{ije_{ij}} : i \in [t], j \in [7], e_{ij} \in [s] \rangle + \langle x_{ijk} : i \in [t], j \in [7], e_{ij} \in [s], k \in [s] \setminus \{e_{ij}\} \rangle + \\ & \langle x_{ijk} \cdot (1 - x_{ijk}) : i \in [t], j \in [7], k \in [s], e_{ij} = 0 \rangle + \langle 1 - \sum_{k \in [s]} x_{ijk} : i \in [t], j \in [7], e_{ij} = 0 \rangle + \\ & \langle x_{ijk} : i \in [t], j \in [7], k \in [s], w_{kj} = 0 \rangle + \langle w_{kj} - \sum_{i \in [t]} x_{ijk} : j \in [7], k \in [s], w_{kj} \neq 0 \rangle. \end{aligned}$$

Moreover,  $|\text{RS}_{W,E}| = \dim_{\mathbb{Q}}(\mathbb{Q}[x_{111}, \dots, x_{t7s}]/I_{W,E})$ .

**Proof.** Any rotating schedule  $R = (r_{ij}) \in \text{RS}_{W,E}$  can be uniquely identified with a zero  $(x_{111}, \dots, x_{t7s})$ , where  $x_{ijk} = 1$  if  $r_{ij} = k$  and 0, otherwise. The finiteness of  $\text{RS}_W$  implies  $I_{W,E}$  to be zero-dimensional. Besides, since  $I_{W,E} \cap \mathbb{Q}[x_{ijk}] = \langle x_{ijk} \cdot (1 - x_{ijk}) \rangle \subseteq I_{W,s,t}$  for all  $i \in [t]$ ,  $j \in [7]$  and  $k \in [s]$ , Proposition 2.7 of [5] assures  $I_{W,E}$  to be radical and thus, Theorem 2.10 of [5] implies that  $|\mathcal{R}_{W,E}| = |V(I_{W,E})| = \dim_{\mathbb{Q}}(\mathbb{Q}[x_{111}, \dots, x_{t7s}]/I_{W,E})$ .  $\square$

Constraints C.3 to C.6 can be imposed to our rotating schedules if we translate them in terms of Boolean polynomials of  $\mathbb{Q}[x_{111}, \dots, x_{t7s}]$ , which can be incorporated to the ideal  $I_{W,E}$ .

C.3) For all  $k \in [s-1]$  and  $l \in [s-1] \setminus \{k\}$ , we add:

$$\begin{cases} x_{ijk} \cdot x_{i(j+1)l}, & \text{for all } i \in [t], j \in [6], \\ x_{i7k} \cdot x_{(i+1)1l}, & \text{for all } i \in [t-1], \\ x_{t7k} \cdot x_{11l}. \end{cases}$$

C.4) For a lower bound of 2 work days, we add, for each  $k \in [s-1]$ :

$$\begin{cases} (x_{ijk} - 1) \cdot x_{i(j+1)k} \cdot (x_{i(j+2)k} - 1), & \text{for all } i \in [t], j \in [5], \\ (x_{i6k} - 1) \cdot x_{i7k} \cdot (x_{(i+1)1k} - 1), & \text{for all } i \in [t-1], \\ (x_{i7k} - 1) \cdot x_{(i+1)1k} \cdot (x_{(i+1)2k} - 1), & \text{for all } i \in [t-1], \\ (x_{t6k} - 1) \cdot x_{t7k} \cdot (x_{11k} - 1), \\ (x_{t7k} - 1) \cdot x_{11k} \cdot (x_{12k} - 1). \end{cases}$$

For an upper bound of 6 work days, we add:

$$\begin{cases} \prod_{j=d}^7 x_{ijk} \cdot \prod_{j=1}^{d-1} x_{(i+1)jk}, & \text{for all } i \in [t-1], d \in [7], k \in [s-1], \\ \prod_{j=d}^7 x_{tjk} \cdot \prod_{j=1}^{d-1} x_{1jk}, & \text{for all } d \in [7], k \in [s-1]. \end{cases}$$

C.5) Similarly to Constraint C.4, we add:

$$\begin{cases} (x_{ijs} - 1) \cdot x_{i(j+1)s} \cdot (x_{i(j+2)s} - 1), & \text{for all } i \in [t], j \in [5], \\ (x_{i6s} - 1) \cdot x_{i7s} \cdot (x_{(i+1)1s} - 1), & \text{for all } i \in [t-1], \\ (x_{i7s} - 1) \cdot x_{(i+1)1s} \cdot (x_{(i+1)2s} - 1), & \text{for all } i \in [t-1] \\ (x_{t6s} - 1) \cdot x_{t7s} \cdot (x_{11s} - 1), \\ (x_{t7s} - 1) \cdot x_{11s} \cdot (x_{12s} - 1). \end{cases}$$

$$\begin{cases} \prod_{j=d}^7 x_{ijs} \cdot \prod_{j=1}^{d-1} x_{(i+1)js}, & \text{for all } i \in [t-1], d \in [7], \\ \prod_{j=d}^7 x_{tjs} \cdot \prod_{j=1}^{d-1} x_{1js}, & \text{for all } d \in [7]. \end{cases}$$

C.6) For all  $k \in \{2, \dots, s-1\}$ ,  $l \in [k-1]$ , we add:

$$\begin{cases} x_{ijk} \cdot x_{i(j+1)l}, & \text{for all } i \in [t], j \in [6], \\ x_{i7k} \cdot x_{(i+1)1l}, & \text{for all } i \in [t-1], \\ x_{t7k} \cdot x_{11l}. \end{cases}$$

### 3 Implementation of the method.

We have considered all the Boolean polynomials of the previous section in order to implement in SINGULAR the procedure *rotating* [3], which determines explicitly the subset of rotating schedules of  $\text{RS}_{W,E}$ , which satisfy some of the Constraints C.1-C.6. It is worth highlighting the effectiveness of this procedure in case of considering rotating schedules related to part time employees for which the initial workload matrix contains zero entries distributed throughout the week. To test it, we have considered the following two workload matrices used by Laporte in [8].

$$w_1 = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 2 & 2 & 2 & 2 \\ 4 & 4 & 2 & 0 & 0 & 1 & 1 \end{pmatrix} \quad w_2 = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 2 & 2 & 2 & 2 \\ 5 & 5 & 3 & 1 & 1 & 2 & 2 \end{pmatrix}$$

According to Constraints C.1 and C.2, we have also imposed that our rotating schedules must contain the following two respective arrays.

$$E_1 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 4 & 4 & 4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \quad E_2 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 4 & 4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 4 & 4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

We show in Table 1 the number of rotating schedules related to the previous arrays, according to the constraints C.3-C.6 which can be imposed. In each case, we also indicate the running time (*r.t.*) in seconds which has been necessary in a system with an *Intel Core i7-2600, 3.4 GHz* and *Ubuntu*. The computational cost of those cases marked by an asterisk has turned out to be excessive for the processing capability of the mentioned computer system.

Constraints				$ \mathcal{RS}_{W_1, E_1} $	r.t.	$ \mathcal{RS}_{W_2, E_2} $	r.t.
C.3	C.4	C.5	C.6				
				15,552	0	648,000	0
x				3	0	360	97
	x			36	0	216	8
		x		15,552	0	145,152	650
			x	81	0	*	*
x	x			3	1	42	4
x		x		3	1	62	14
x			x	3	1	71	93
	x	x		36	1	48	7
		x	x	9	1	360	13
			x	81	1	*	*
x	x	x		3	1	10	3
x	x		x	3	1	42	6
x		x	x	3	1	62	15
	x	x	x	9	1	30	8
x	x	x	x	3	1	10	5

Table 1: Distribution of rotating schedules according to the type of constraints.

The three rotating schedules related to  $W_1$  and  $E_1$  which satisfies all the constraints are:

$$\begin{pmatrix} 4 & 4 & 4 & 3 & 3 & 3 & 3 \\ 4 & 4 & 2 & 2 & 2 & 4 & 4 \\ 4 & 4 & 4 & 3 & 3 & 3 & 3 \\ 4 & 4 & 4 & 1 & 1 & 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 4 & 4 & 4 & 3 & 3 & 3 & 3 \\ 4 & 4 & 2 & 2 & 2 & 4 & 4 \\ 4 & 4 & 4 & 1 & 1 & 1 & 1 \\ 4 & 4 & 4 & 3 & 3 & 3 & 3 \end{pmatrix}, \quad \begin{pmatrix} 4 & 4 & 1 & 1 & 1 & 1 & 1 \\ 4 & 4 & 2 & 2 & 2 & 4 & 4 \\ 4 & 4 & 4 & 3 & 3 & 3 & 3 \\ 4 & 4 & 4 & 3 & 3 & 3 & 3 \end{pmatrix}.$$

The ten rotating schedules related to  $W_2$  and  $E_2$  which satisfy all the constraints are:

$$\begin{pmatrix} 4 & 4 & 4 & 4 & 4 & 3 & 3 \\ 4 & 4 & 4 & 3 & 3 & 4 & 4 \\ 4 & 4 & 4 & 3 & 3 & 3 & 3 \\ 4 & 4 & 2 & 2 & 2 & 4 & 4 \\ 4 & 4 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 4 & 4 & 4 & 4 & 4 & 3 & 3 \\ 4 & 4 & 2 & 2 & 2 & 4 & 4 \\ 4 & 4 & 4 & 3 & 3 & 3 & 3 \\ 4 & 4 & 4 & 3 & 3 & 4 & 4 \\ 4 & 4 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 4 & 4 & 4 & 3 & 3 & 3 & 3 \\ 4 & 4 & 1 & 1 & 4 & 4 & 4 \\ 4 & 4 & 4 & 3 & 3 & 3 & 3 \\ 4 & 4 & 2 & 2 & 2 & 4 & 4 \\ 4 & 4 & 4 & 4 & 1 & 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 4 & 4 & 4 & 3 & 3 & 3 & 3 \\ 4 & 4 & 2 & 2 & 2 & 4 & 4 \\ 4 & 4 & 4 & 4 & 1 & 1 & 1 \\ 4 & 4 & 4 & 3 & 3 & 3 & 3 \\ 4 & 4 & 4 & 3 & 3 & 3 & 3 \end{pmatrix}, \quad \begin{pmatrix} 4 & 4 & 4 & 4 & 1 & 1 & 1 \\ 4 & 4 & 2 & 2 & 2 & 4 & 4 \\ 4 & 4 & 4 & 3 & 3 & 3 & 3 \\ 4 & 4 & 1 & 1 & 4 & 4 & 4 \\ 4 & 4 & 4 & 3 & 3 & 3 & 3 \end{pmatrix},$$

$$\begin{pmatrix} 4 & 4 & 4 & 4 & 4 & 3 & 3 \\ 4 & 4 & 2 & 2 & 2 & 4 & 4 \\ 4 & 4 & 1 & 1 & 1 & 1 & 1 \\ 4 & 4 & 4 & 3 & 3 & 4 & 4 \\ 4 & 4 & 4 & 3 & 3 & 3 & 3 \end{pmatrix}, \quad \begin{pmatrix} 4 & 4 & 4 & 4 & 4 & 1 & 1 \\ 4 & 4 & 2 & 2 & 2 & 4 & 4 \\ 4 & 4 & 4 & 3 & 3 & 3 & 3 \\ 4 & 4 & 1 & 1 & 1 & 1 & 1 \\ 4 & 4 & 4 & 3 & 3 & 3 & 3 \end{pmatrix}, \quad \begin{pmatrix} 4 & 4 & 4 & 4 & 4 & 3 & 3 \\ 4 & 4 & 4 & 3 & 3 & 4 & 4 \\ 4 & 4 & 1 & 1 & 1 & 1 & 1 \\ 4 & 4 & 2 & 2 & 2 & 4 & 4 \\ 4 & 4 & 4 & 3 & 3 & 3 & 3 \end{pmatrix}, \quad \begin{pmatrix} 4 & 4 & 4 & 4 & 4 & 1 & 1 \\ 4 & 4 & 1 & 1 & 1 & 4 & 4 \\ 4 & 4 & 4 & 3 & 3 & 3 & 3 \\ 4 & 4 & 2 & 2 & 2 & 4 & 4 \\ 4 & 4 & 4 & 3 & 3 & 3 & 3 \end{pmatrix}.$$

The number of possible rotating schedules in Table 1 may also give us information about the influence of each constraint on the final schedule. Thus, for instance, we can observe how Constraint C.5 does not have any influence on the design of a rotating schedule of workload matrix  $W_1$ , i.e., it does not diminishes the number of solutions when it is considered alone neither in combination with other constraints. However, it can be observed that it has influence on the design of rotating schedules of workload matrix  $W_2$ .

## 4 Final remarks and further work.

In the current paper, we have shown how the polynomial method can be used in order to determine explicitly all the possible rotating schedules which satisfy a given set of constraints and to analyze their influence on the existence of such schedules. Besides, we have just seen in Table 1 that, depending on the constraints in which we are interested, the computational cost which is necessary to obtain a rotating schedule can be excessive even for small orders. A possible alternative to be considered as further work is to construct such a schedule by using the *column generation* method [9], which consists of determining all the shifts of one day, before of obtaining those of the following day. The number of variables which is necessary to use in such a case is considerably reduced and hence, the computational cost is improved.

## References

- [1] H. K. Alfares, Survey, Categorization, and Comparison of Recent Tour Scheduling Literature, *Annals of Operations Research* 127 (2004) no. 1-4, 145–175.
- [2] N. Alon, Combinatorial Nullstellensatz, Recent trends in combinatorics (Mátraháza, 1995). *Combin. Probab. Comput.* 8 (1999) no. 1–2, 7–29.
- [3] E. Barrena, D. Canca and R. M. Falcón, <http://personal.us.es/raufalgan/LS/crew.lib>.
- [4] A. Bernasconi, B. Codenotti, V. Crespi and G. Resta, Computing Groebner Bases in the Boolean Setting with Applications to Counting, 1st Workshop on Algorithm Engineering (WAE). Venice, Italy, 1997, pp. 209–218.
- [5] D. A. Cox, J. B. Little and D. O’Shea, *Using Algebraic Geometry*, Springer-Verlag, New York, 1998.
- [6] W. Decker, G.-M. Greuel, G. Pfister and H. Schönemann, SINGULAR 3-1-6. A computer algebra system for polynomial computations, 2013. <http://www.singular.uni-kl.de>.
- [7] M. Gamache, A. Hertz and J. O. Ouellet, A graph coloring model for a feasibility problem in monthly crew scheduling with preferential bidding, *Computers & OR* 34 (2007) no. 8, 2384–2395.
- [8] G. Laporte, The art and science of designing rotating schedules, *Journal of the Operational Research Society* 50 (1999) no. 10, 1011–1017.
- [9] G. Laporte and G. Pesant, A general multi-shift scheduling system, *Journal of the Operational Research Society* 55 (2004) no. 11, 1208–1217.
- [10] J. A. Loera, J. Lee, S. Margulies and S. Onn, Expressing Combinatorial Problems by Systems of Polynomial Equations and Hilberts Nullstellensatz, *Combinatorics, Probability and Computing* 18 (2009) 551–582.
- [11] J. A. De Loera, C. J. Hillar, P. N. Malkin and M. Omar, Recognizing Graph Theoretic Properties with Polynomial Ideals, *Electron. J. Combin.* 17 (2010) no. 1, Research Paper 114, 26 pp.

# Simulating Car Traffic with Smart Signals using a CAS

José Luis Galán, Gabriel Aguilera, José Carlos Campos, Pedro Rodríguez  
University of Málaga (Spain)

`jl_galan@uma.es`

## Abstract

Smart cities designs involve different characteristics, being the use of smart traffic lights and smart signals two of the most important ones. One of the greatest problems to deal with is that any physical implementation of these smart traffic signals are expensive in both, money and resources.

Therefore, any virtual implementation of such signals within a traffic structure can provide important information in order to test the behavior of different designs previously to a physical implementation.

In this talk, we present a model which allow accelerated-time simulations of car traffic using smart signals in a city. The implementation of the model has been developed using MAXIMA. The use of this CAS enable the use of different probability distributions for the different controlled aspects including the possibility of defining an ad-hoc distribution which can fit better the user necessities for the simulation. The use of a CAS is needed mainly because in order to deal with an ad-hoc distribution, exact and symbolic computations are required (for example, for antiderivatives computation). On the other hand, when using a CAS with classical probability distributions, such as exponential distribution, Poisson distribution or normal distribution, exact computations produce better results than when approximating the generated values for such distributions.

In order to easily follow the simulation, a graphical approach of the model has been also developed using Java. This combination of Java and Maxima allows also to have a portable implementation of the model which can run in most computer systems.

Finally, this work is part of the future work stated in previous works on accelerated-time simulations presented in ACA'11 and ACA'12 also in the Nonstandard Session.

## References

- [1] GABRIEL AGUILERA AND JOSÉ LUIS GALÁN AND JOSÉ MANUEL GARCÍA AND ENRIQUE MÉRIDA AND PEDRO RODRÍGUEZ. An accelerated-time simulation of car traffic on a motorway using a CAS. *Math. Comput. Simul.* (2012), <http://dx.doi.org/10.1016/j.matcom.2012.03.010>.

## Keywords

Accelerated-time simulation, Smart cities, Smart signals, CAS

# Padovan-like sequences and Bell polynomials

Nikita Gogin

Åbo Akademi University (Finland)

Aleksandr Mylläri

St. George's University (Grenada)

amyllari@sgu.edu

## Abstract

We study a class of Padovan-like sequences that can be generated using special matrices of the third order. We show that terms of any sequence of this class can be expressed via Bell polynomials and their derivatives that use as arguments terms of another such sequence with smaller indexes. *CAS Mathematica* is used for cumbersome calculations and hypothesis testing.

## Keywords

Padovan sequence, Fibonacci numbers, Bell polynomials, integer sequences

## 1 Introduction

Integer sequences appear in many branches of science. One famous example is Fibonacci numbers that have been known for more than two thousand years and find applications in mathematics, biology, economics, computer science. Padovan numbers are much younger - they were introduced only recently [1]. Below, we will study Padovan-like sequences that can be generated using special matrices of the third order. We will find expressions for terms of one sequence in terms of another sequence via Bell polynomials. *CAS Mathematica* was used for cumbersome calculations and hypothesis testing.

Let

$$A_\alpha = \begin{pmatrix} 0 & \alpha & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

and let  $\begin{pmatrix} u_n \\ v_n \\ w_n \end{pmatrix}$  for a time denote the first column of  $A_\alpha^n$ ,  $n \geq 0$ . Then

$$u_{n+1} = \alpha v_n + w_n, \quad v_{n+1} = u_n, \quad w_{n+1} = v_n. \quad (1)$$

We have

$$u_{n+1} = \alpha u_{n-1} + u_{n-2}, \quad u_0 = 1, \quad u_1 = 0, \quad u_2 = \alpha, \quad (u_{-1} = 0,) \quad (2)$$

$$A_\alpha^n = \begin{pmatrix} u_n & u_{n+1} & u_{n-1} \\ u_{n-1} & u_n & u_{n-2} \\ u_{n-2} & u_{n-1} & u_{n-3} \end{pmatrix}. \quad (3)$$

Some examples of sequences generated by the matrix  $A_\alpha$  with references to the On-Line Encyclopedia of Integer Sequences (OEIS, <http://oeis.org/>) are given in Table 1.



Table 1: Examples of sequences generated by the matrix  $A_\alpha$ .

$\alpha$	OEIS reference	First terms	Comment
$\alpha = 1$	A000931	1,0,1,1,1,2,2,3,4,5,7,9,12,16,21,	Padovan sequence : $u_n = p_n$
$\alpha = 2$	A008346	1,0,2,1,4,4,9,12,22,33,56,88,145,	$u_n = f_n = \text{Fibonacci}(n) + (-1)^n$
$\alpha = 3$	A052931	1,0,3,1,9,6,28,27,90,109,297,417,	
$\alpha = 0$	A079978	1,0,0,1,0,0,1,0,0,1,0,0,1,0,0, 1,	$u_n = t_n = \begin{cases} 1, & n \equiv 0(\text{mod } 3) \\ 0, & n \equiv 1, 2(\text{mod } 3) \end{cases}$ $= \binom{\frac{n}{3}}{0}$
$\alpha = -1$	A077961	1,0,-1,1,1,-2,0,3,-2,-3,5,1,-8,4,9,	
$\alpha = -2$	A077965	1,0,-2,1,4,-4,-7,12,10,-31,-8,72,-15,-152,102	

## 2 Main Result

Now let  $\beta \in Z$ , and let  $v_n$  denote terms of the sequence corresponding to the powers of the matrix  $A_\beta$ , and let  $w_n$  denote terms of the sequence corresponding to the powers of the matrix  $A_{\alpha+\beta}$  :

$$A_{\alpha+\beta}^n = \begin{pmatrix} w_n & w_{n+1} & w_{n-1} \\ w_{n-1} & w_n & w_{n-2} \\ w_{n-2} & w_{n-1} & w_{n-3} \end{pmatrix} = \begin{pmatrix} 0 & \alpha + \beta & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}^n = (A_\alpha + \beta e)^n = (A_\beta + \alpha e)^n,$$

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

Terms of the sequence generated by  $A_{\alpha+\beta}$  can be expressed in terms of the sequence generated by  $A_\alpha$  as follows:

$$w_n = \sum_{\varepsilon=0}^1 \sum_{s=1}^{\lfloor \frac{n+\varepsilon}{2} \rfloor} \frac{(s-\varepsilon)! \cdot \beta^{s-\varepsilon}}{(n-s+\varepsilon)!} \times \mathcal{D}^\varepsilon (B_{n-s+\varepsilon, s}(1! \cdot u_{k_1-1}, 2! \cdot u_{k_2-1}, \dots, (n-2s+1+\varepsilon)! \cdot u_{k_{n-2s+1+\varepsilon}-1})), \quad (4)$$

where  $k_i$  run over all partitions of  $n-s+\varepsilon$  into  $s$  parts,  $\mathcal{D}^0 = id$  - identity operator,  $\mathcal{D}^1 = \mathcal{D} = \sum_{r=1}^{(\infty)} x_{r+1} \frac{\partial}{\partial x_r}$ , and

$$B_{n,k}(x_1, x_2, \dots, x_{n-k+1}) = \sum \frac{n!}{j_1! j_2! \dots j_{n-k+1}!} \left(\frac{x_1}{1!}\right)^{j_1} \left(\frac{x_2}{2!}\right)^{j_2} \dots \left(\frac{x_{n-k+1}}{(n-k+1)!}\right)^{j_{n-k+1}} \quad (5)$$

are partial Bell polynomials, and summing is done for all sets  $j_1, j_2, \dots, j_{n-k+1}$  of non-negative integers such that  $j_1 + j_2 + \dots + j_{n-k+1} = k$  and  $1 \cdot j_1 + 2 \cdot j_2 + 3 \cdot j_3 + \dots + (n-k+1) \cdot j_{n-k+1} = n$  (see [2]).

### 3 Examples

#### 3.1 Example 1

For  $\alpha = \beta = 1$  formula (4) gives a relation between terms of Fibonacci and Padovan sequences:

$$\begin{aligned} f_n &= \text{Fibonacci}(n) + (-1)^n = \\ &= \sum_{\varepsilon=0}^1 \sum_{s=1}^{\lfloor \frac{n+\varepsilon}{2} \rfloor} \frac{(s-\varepsilon)!}{(n-s+\varepsilon)!} \mathcal{D}^\varepsilon(B_{n-s+\varepsilon,s}(1! \cdot p_{k_1-1}, 2! \cdot p_{k_2-1}, \dots, (n-2s+1+\varepsilon)! \cdot p_{k_{n-2s+1+\varepsilon}-1})), \end{aligned} \quad (6)$$

and thus for  $n \geq 1$  the  $n$ -th term of the sequence  $\text{Fibonacci}(n) + (-1)^n$  is expressed as sums of products of the  $n$  first terms of the Padovan sequence.

#### 3.2 Example 2

For  $\alpha = 2$  and  $\beta = -2$  formula (4) gives a relation between terms of sequences  $f_n = \text{Fibonacci}(n) + (-1)^n$  and  $t_n = \begin{cases} 1, & n \equiv 0 \pmod{3} \\ 0, & n \equiv 1, 2 \pmod{3} \end{cases}, n \geq 1$ :

$$\begin{aligned} \sum_{\varepsilon=0}^1 \sum_{s=1}^{\lfloor \frac{n+\varepsilon}{2} \rfloor} \frac{(s-\varepsilon)!(-2)^{s-\varepsilon}}{(n-s+\varepsilon)!} \mathcal{D}^\varepsilon(B_{n-s+\varepsilon,s}(1! \cdot f_{k_1-1}, 2! \cdot f_{k_2-1}, \dots, (n-2s+1+\varepsilon)! \cdot f_{k_{n-2s+1+\varepsilon}-1})) = \\ = \begin{cases} 1, & n \equiv 0 \pmod{3} \\ 0, & n \equiv 1, 2 \pmod{3} \end{cases} \quad (7) \end{aligned}$$

#### 3.3 Example 3

In particular, the terms of every Padovan-like sequence with  $\alpha \neq 0$  can be expressed in the same way via the terms of the "simplest generator" of the class, namely the sequence 1, 0, 0, 1, 0, 0, 1, 0, 0, ... generated by  $\alpha = 0$  (OEIS-number A079978, see Table 1). This statement is a far-reaching generalization of the result announced by J. Vladetta in [3].

### References

- [1] Richard Padovan, Dom Hans Van Der Laan and the Plastic Number, pp. 181-193 in *Nexus IV: Architecture and Mathematics*, eds. Kim Williams and Jose Francisco Rodrigues Fucecchio (Florence): Kim Williams Books, 2002.
- [2] [http://en.wikipedia.org/wiki/Bell\\_polynomials](http://en.wikipedia.org/wiki/Bell_polynomials)
- [3] Vladetta.J , in "Sloane's A000931 : Padovan sequence", The On-Line Encyclopedia of Integer Sequences. OEIS Foundation.

# Modeling reliability in propositions using computer algebra techniques

Antonio Hernando  
Universidad Politécnica de Madrid (Spain)

ahernando@eui.upm.es

## Abstract

We present an algebraic method designed to deal with with reliability in propositional logic. Our approach may be regarded as an extension of classical bivalued propositional logics, in which each propositional formula is assigned a certain degree of unreliability. According to this approach, each formula will be used in the context of reasoning depending on how much reliability it is associated with. The more reliable a formula is, the more likely will it be employed in order to get a logical conclusion. This approach involves a quite different concept to that of probabilistic logics, since the logical notions of tautological consequence and consistency of a set of formulae are reformulated on behalf of the foreseen unreliability values. Here we state a relation between these unreliability values associated to tautological consequence and the calculation of reduced Groebner bases on an ideal of Boolean polynomials. In this way, our method for assigning these unreliability values to information and reasoning turns out to have a straightforward translation into algebraic terms. Thus, any knowledge system using our model can be implemented in a mathematical program, like Maple, CoCoA or specialized software on Boolean polynomials like Polybori. This work is related to the algebraic approaches used for multivalued logics. However, these algebraic approaches result to be impractical since they deal with polynomials of high degree. Otherwise, since our approach involves only Boolean polynomials, we think that this may be interesting for implementing expert system managing uncertainty information.

## Keywords

Expert Systems, Boolean logic, Groebner Basis

## 1 Introduction

This paper presents an algebraic method for considering uncertainty on knowledge described by Boolean propositional logic. This may be regarded as an refinement of the model presented in [15]. Unlike the algebraic model presented previously, we here present an algebraic model which involves only Boolean polynomials. This fact implies an important advantage above the previous one, since we improve the efficiency of inference under uncertainty by means of specialized software on Boolean polynomials (like Polybori) which runs much faster than a non-specialized computer algebra system.

This work may be related to the algebraic approaches used for multivalued logics. Nevertheless, these algebraic approaches are impractical since they deal with polynomials of high degree. Otherwise, since our approach involves only Boolean polynomials, we think that this may be interesting for implementing expert systems managing uncertainty information. As an example, we have implemented our approach using the CAS CoCoA.

## 2 Reasoning with unreliability

In this section, we will consider formal definitions involved in our model, which were presented in [15].

**Definition 1** (Formula). Let  $X_1, \dots, X_m$  be variables. A formula is defined recursively as follows:

- $X_i$ , where  $X_i \in X_1, \dots, X_m$  is a variable (also usually called a proposition)

- $\neg B$ , where  $B$  is a formula
- $B \vee C$ , where  $B$  and  $C$  are formulae

Each formula in our model is associated to a certain unreliability degree, indicating how dubious the information contained in that formula is to the knowledge system. This unreliability degree can go from 0 to  $2^n - 1$ , where  $n$  is any natural number. Throughout this paper, we will use letter  $q$  referring to  $2^n$ , being the number of possible unreliability degrees we can assign to any formula. In this way, the definition of an unreliable formula runs as follows:

**Definition 2** (Unreliable formula). Let  $X_1, \dots, X_m$  be variables. An unreliable formula is a formula  $A$  along with a value  $g(A) \in \mathbb{N}$ , such that  $0 \leq g(A) \leq q$ .

We will make use of  $\mathcal{C}$  to denote the set of unreliable formulae.

**Definition 3** (Valuation). Let  $A \in \mathcal{C}$ . Let  $x_1^*, \dots, x_m^* \in \{0, 1\}$ , a valuation of the formula  $A$ ,  $A(x_1^*, \dots, x_m^*)$ , is defined recursively as follows:

- If  $A \equiv X_i$ , then  $A(x_1^*, \dots, x_m^*) = x_i^*$
- If  $A \equiv \neg B$ , then we have that

$$A(x_1^*, \dots, x_m^*) = \begin{cases} 1 & \text{if } B(x_1^*, \dots, x_m^*) = 0 \\ 0 & \text{otherwise} \end{cases}$$

- If  $A \equiv B \vee C$ , then

$$A(x_1^*, \dots, x_m^*) = \begin{cases} 1 & \text{if } B(x_1^*, \dots, x_m^*) = 1 \\ 1 & \text{if } C(x_1^*, \dots, x_m^*) = 1 \\ 0 & \text{otherwise} \end{cases}$$

**Remark 1.** We will say that a formula  $A$  holds for a valuation  $(x_1^*, \dots, x_m^*)$  if and only if  $A(x_1^*, \dots, x_m^*) = 1$ .

In classic propositional logic, a set of formulae is said to be consistent if it is possible that all these formulae hold for a valuation. Now, we will generalize this concept for unreliable formulae. A set of unreliable formulae is said to be consistent to a certain degree,  $v$ , ( $v$ -consistent) if the subset of formulae with an unreliability degree equal or lesser than  $v$  is consistent in the usual sense of classical logic.

**Definition 4** (Consistent). Let  $0 \leq v \leq q$ .

Let  $A_1, \dots, A_r \in \mathcal{C}$ .

$\{A_1, \dots, A_r\}$  is  $v$ -consistent  $\Leftrightarrow \exists x_1^*, \dots, x_m^* \in \{0, 1\}$  such that:

$$\text{if } A_i \in \{A_1, \dots, A_r\} \text{ and } g(A_i) \leq v, \text{ then } A_i(x_1^*, \dots, x_m^*) = 1$$

Next we will provide a generalization of the notion of tautological consequence in terms of our model. As was the case with the concept of consistence, we will reach a redefinition of tautological consequence as applied to unreliable formulae. An unreliable formula,  $B$ , is said to be a tautological consequence to a certain degree,  $v$ , of a set of formulae ( $v$ -tautological consequence) when  $B$  is a tautological consequence (in the usual sense of classic propositional logic) of the subset of formulae with an unreliability degree equal or lesser than  $v$ .

**Definition 5** (Tautological Consequence). Let  $0 \leq v \leq q$ .

Let  $A_1, \dots, A_r, B \in \mathcal{C}$ .

$B$  is a  $v$ -tautological consequence of  $\{A_1, \dots, A_r\}$  if and only if  $\forall x_1^*, \dots, x_m^* \in \{0, 1\}$  the following holds:

if  $\forall A_i \in \{A_1, \dots, A_r \mid g(A_i) \leq v\} A_i(x_1^*, \dots, x_m^*) = 1$ , then  $B(x_1^*, \dots, x_m^*) = 1$ .

**Remark 2.**  $B$  is a  $v$ -tautological consequence of  $\{A_1, \dots, A_r\}$  independently of the unreliability degree of  $B$ ,  $g(B)$ .

### 3 Algebraic approach

In this section we will focus on the procedure to translating logical formulae into polynomials, we will study some properties about the resulting polynomials, while analyzing the relation between such polynomials and the logical formulae they stand for.

First of all, we will define the ideal (in order to define Boolean polynomials):

**Definition 6** (Ideal  $J$ ). We define the following ideal in  $\mathbb{Z}_2[x_1, x_2, \dots, x_m, y_1, \dots, y_q]$

$$J = \langle x_1^2 + x_1, x_2^2 + x_2, \dots, x_m^2 + x_m, y_1^2 + y_1, \dots, y_q^2 + y_q \rangle$$

We will associate a polynomial in  $\mathbb{Z}_2[x_1, x_2, \dots, x_m, y_1, \dots, y_q]$  to each unreliable formula in  $\mathcal{C}$ . This will enable us to focus in an algebraic way the problem of determining the consistency degree of a set of unreliable formulae and the deduction degree of an unreliable formula as derived from others.

In our translating procedure we make use of a normal form, NF, of the polynomials on the ideal  $J$ . The use of the normal form interests us because it produces ‘simpler’ polynomials. Prior to translating formulae affected by unreliability values, we will define the translation into polynomials of single formulae with no associated unreliability degrees.

**Definition 7** (polynomial of a formula). Let  $A \in \mathcal{C}$ . The polynomial associated to the formula  $A$ ,  $q_A \in \mathbb{Z}_2[x_1, \dots, x_m]$ , is recursively defined as follows:

- If  $A \equiv X_i$ , where  $X_i$  is a variable, then  $q_A = x_i$
- If  $A \equiv \neg B$ , then  $q_A = \text{NF}(q_B + 1, J)$
- If  $A \equiv B \vee C$ , then  $q_A = \text{NF}(q_B \cdot q_C, J)$

**Remark 3.** The polynomial  $q_A$  associated to the formula  $A$  is defined regardless of the unreliability degree of the formula  $A$ ,  $g(A)$ .

Next, on the basis of Definition 7, we define another kind of polynomials associated to each unreliable formula, but also taking into account the unreliability degree of the formulae. These polynomials will be helpful for determining the consistency degree of formulae and the deduction degree as derived from others.

**Definition 8** (polynomial of an unreliable formula). Given an unreliable formula  $A \in \mathcal{C}$  such that  $g(A) = v$ , the polynomial associated to the unreliable formula  $A$ ,  $p_A \in \mathbb{Z}_2[x_1, \dots, x_m, y_1, \dots, y_n]$ , is defined as follows:

$$p_A = q_A \cdot y_1 y_2 \cdot y_v$$

**Remark 4.** Since the normal form is here used, the indeterminates  $x_1, \dots, x_m, y_1, \dots, y_q$  are never to a power greater than 1.

**Remark 5.** When the unreliability degree of a formula  $A$  is 0, that is to say,  $g(A) = 0$ , then  $p_A = q_A$ .

Next, we will present the main result of this paper:

**Theorem 1.** Let  $A_1, \dots, A_r, C \in \mathcal{C}$ .

We have that:

- $B$  is  $v$ -tautological consequence of  $\{A_1, \dots, A_r\} \Leftrightarrow y_1 \dots y_v \cdots q(B) \in \langle q(A_1) \dots q(A_r) \rangle$
- $\{A_1, \dots, A_r\}$  is  $v$ -consistent  $\Leftrightarrow y_1 \dots y_v \notin \langle q(A_1) \dots q(A_r) \rangle$

According to the previous result, any knowledge system managing uncertainty on Boolean propositional can be implemented in a computer algebra system, like CoCoA or Polybori.

### Acknowledgment

This work was partially supported by the research projects TIN2012-32682 (Ministerio de Educación y Ciencia, Spain).

## 4 Conclusions

In this paper we have presented an algebraic model for managing knowledge affected by different degrees of unreliability. This model may be regarded as an extension on classical propositional logics, with addition of unreliability values associated to each proposition. The usual logical notions of tautological consequence and consistency of a given set of formulae have been redefined on behalf of the unreliability values. The main contribution of this work is concerned with the link between the unreliability values associated to tautological consequence and the calculation of reduced Groebner bases on an ideal of polynomials.

## References

- [1] J. A. Alonso, E. Briales, Lógicas Polivalentes y Bases de Gröbner. In: C. Martin (ed.), *Actas del V Congreso de Lenguajes Naturales y Lenguajes Formales*. University of Seville, Seville, 1995, pp. 307-315.
- [2] T. Becker, V. Weisspfenning, *Gröbner bases. A computational approach to commutative algebra*, Berlin, Graduate Studies in Mathematics-Springer, 1993.
- [3] B. Buchberger: *An Algorithm for Finding a Basis for the Residue Class Ring of a Zero-Dimensional Polynomial Ideal* (Ph.D. Thesis in German). Math. Institute - University of Innsbruck, 1965.
- [4] B. Buchberger, *Applications of Gröbner Bases in Non-Linear Computational Geometry*. In: J. R. Rice (ed.), *Mathematical Aspects of Scientific Software*. Springer-Verlag, New York, 1988, pp. 60-88.
- [5] A. Capani, G. Niesi, *CoCoA Users Manual v. 3.0b*, Genova, Department of Mathematics, University of Genova, 1996: See CoCoA, 2004 <http://cocoa.dima.unige.it>.
- [6] J. Chazarain, A. Riscos, J. A. Alonso, E. Briales, *Multivalued Logic and Gröbner Bases with Applications to Modal Logic*, *Journal of Symbolic Computation* 11 (1991) 181-194.
- [7] G. de Cooman, F. Hermans, *Imprecise probability trees: Bridging two theories of imprecise probability*, *Artificial Intelligence* 172 (2008) 1400-1427.
- [8] D. Cox, J. Little, D. O'Shea, *Ideals, Varieties, and Algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra*, Springer, New York, 1992.
- [9] F. G. Cozman, C. P. de Campos, J. C. Ferreira da Rocha, *Probabilistic logic with independence*, *Int. Journ. Approximate Reasoning* 49 (2008) 3-17.
- [10] J. C. Faugère, *A new efficient algorithm for computing Gröbner bases without reduction to zero*. In: T. Mora (ed.), *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation (ISSAC 2002)*, ACM Press, 2002, pp. 75-83.
- [11] V. P. Gerdt, M. V. Zinin, *A Pommaret Division Algorithm for Computing Gröbner Bases in Boolean Rings*. In: J. R. Sendra, L. Gonzalez-Vega (eds.), *Symbolic and Algebraic Computation, International Symposium ISSAC 2008*, ACM Press, 2008, pp. 95-102.
- [12] G. Gerla, *Inferences in Probability Logic*, *Artificial Intelligence* 70(1-2) (1994) 33-52.
- [13] P. Hansen, B. Jaumard, *Probabilistic satisfiability*, Report G-96-31. Les Cahiers du GERAD, École Polytechnique de Montréal, 1996.
- [14] J. Hsiang, *Refutational Theorem Proving using Term-Rewriting Systems*, *Artificial Intelligence* 25 (1985) 255-300.
- [15] A. Hernando, E. Roanes-Lozano, J. Montero, *An algebraic method for managing reliability in propositional logic*, In: *Proceedings of the 2010 International Conference on Intelligent Systems and Knowledge Engineering (ISKE)*, 2010, pp. 147-152.
- [16] A. Hernando, E. Roanes-Lozano, L.M. Laita: *A Polynomial Model for Logics with a Prime Power Number of Truth Values*. *Journal of Automated Reasoning* 46 (2011), pp. 205-221.

- [17] D. Kapur, P. Narendran, An Equational Approach to Theorem Proving in First-Order Predicate Calculus. In: Proceedings of the 9th International Joint Conference on Artificial Intelligence (IJCAI-85), vol. 2, 1985, pp. 1146-1153.
- [18] P. Krause, D. Clark, Representing Uncertain Knowledge, Kluwer, Dordrecht, 1993.
- [19] L.M. Laita, E. Roanes-Lozano, V. Maojo, L. de Ledesma, L. Laita: An Expert System for Managing Medical Appropriateness Criteria Based on Computer Algebra Techniques. Computers and Mathematics with Applications 51/5 (2000) 473-481.
- [20] T. Lukasiewicz, Probabilistic deduction with conditional constraints over basic events, Journal of Artificial Intelligence Research 10 (1999) 199-241.
- [21] T. Lukasiewicz, Weak nonmonotonic probabilistic logics, Artificial Intelligence 168 (2005) 119-161.
- [22] T. Lukasiewicz, Expressive probabilistic description logics, Artificial Intelligence 172 (2008) 852-883.
- [23] N. J. Nilsson, Probabilistic logic, Artificial Intelligence 28 (1986) 71-87.
- [24] J. Pearl, Probabilistic Reasoning in Intelligent Systems, Morgan Kaufman, San Mateo (CA), 1988.
- [25] C. Pérez-Carretero, L.M. Laita, E. Roanes-Lozano, L. Lázaro, J. González-Cajal, L. Laita, A Logic and Computer Algebra-Based Expert System for Diagnosis of Anorexia, Mathematics and Computers in Simulation 58 (2002) 183-202.
- [26] D. Perkinson, (2000). CoCoA 4.0 online help (electronic file accompanying CoCoA v.4.0).
- [27] P. Walley, Measures of uncertainty in expert systems, Artificial Intelligence 83 (1996) 1-58.
- [28] P. Walley, Towards a unified theory of imprecise probability, Int. Jour. Approximate Reasoning 24 (2000) 125-148.
- [29] Winkler, F., Polynomial algorithms in computer algebra, Springer, Vienna, 1996.

# Flexibility of Structures via Computer Algebra

Robert H. Lewis  
Fordham University (U.S.A.)

Evangelos Coutsias  
University of New Mexico (U.S.A.)  
rlewis@fordham.edu

## Abstract

We solve systems of multivariate polynomial equations in order to understand flexibility of objects in two or three dimensions, including protein-like molecules.

Protein flexibility is a major research topic in computational chemistry. In general, a molecule can be modeled as a polygonal structure whose edges and angles are fixed while some of the dihedral angles can vary freely. One needs to determine mathematically if such a structure is flexible. This can be reduced to the analysis of a system of polynomial equations. Resultant methods have been applied successfully to this problem [3].

In this work we focus on non-generically flexible structures (picture a geodesic dome) that are rigid but become continuously movable under certain relations. The subject has a long history: Cauchy (1812) [2], Bricard (1896) [1], Connelly (1978).

In our previous works [4, 5] we began a new approach to understanding flexibility, using not numeric but symbolic computation. We describe the geometry of the object with a set of multivariate polynomial equations, which we solve with resultants. Resultants were pioneered by Bezout, Sylvester, Dixon, and others. Given the resultant, we described an algorithm *Solve* that examines it and determines relations for the structure to be flexible. We discovered in this way conditions for flexibility of an arrangement of quadrilaterals in Bricard [1] which models molecules and is directly applicable to cyclohexane. In previous works [5], we have shown that the algorithm can be significantly extended to other molecular structures.

In spite of that success, key questions remained. Bricard asserted that there are three ways the configuration of quadrilaterals can be flexible, though there are gaps in his proof. Until recently, our computer programs found only two of them. By the spring of 2012, the revised and streamlined programs found an example of the third case, but not the most general third case. The program now finds that case. Furthermore, we now have a computer-assisted mathematical proof that all cases have been found, thereby completing Bricard's argument. This appears to be the first fully algebraic approach for flexibility.

This has great significance, as we now have confidence that the software is capable of fully analyzing more complex structures, such as cyclooctane.

## References

- [1] Bricard, Raoul, Mémoire sur la théorie de l'octaèdre articulé, J. Math. Pures Appl. 3 (1897), p. 113 - 150  
(English translation: <http://www.math.unm.edu/~vageli/papers/bricard.pdf>).
- [2] Cauchy, A. L. Sur les polygones et les polyèdres. Second Memoire. Journal de l'École Polytechn. 9 (1813), pp. 8.
- [3] Coutsias, E. A., C. Seok, M. J. Wester and K. A. Dill, Resultants and loop closure, Int. J. Quantum Chem. 106 (2005), no. (1), p. 176 - 189.
- [4] Lewis, R. H. and E. A. Coutsias, Algorithmic Search for Flexibility Using Resultants of Polynomial Systems; in Automated Deduction in Geometry, 6th International Workshop, ADG 2006. Springer-Verlag. LNCS 4869 p. 68 - 79 (2007).
- [5] Lewis, Robert H. *Determining Flexibility of Molecules Using Resultants of Polynomial Systems*, ACA Conference, Montreal, Canada, June 25 - 29, 2009.

## Keywords

polynomial systems, resultants, flexibility, protein folding



# A hybrid expert system for classic car recognition and originality evaluation

Eugenio Roanes-Lozano  
Instituto de Matemática Interdisciplinar (IMI),  
Departamento de Álgebra, Facultad de Educación,  
Universidad Complutense de Madrid, E-28040 Madrid (Spain)

Jesús Bonilla  
Motor Clásico magazine (Editor in Chief)  
c/ Ancora 40, E-28045 Madrid (Spain)

`eroanes@mat.ucm.es`

## Abstract

Apart from the condition of the car, one of the main problems when buying a classic car (or when estimating its value) is recognizing its originality.

Many times, non-original parts and accessories have been installed, what is not normally very difficult to find out. But sometimes items from other versions of the same model can be found in a certain specimen, what is not that easy to recognize.

We have developed in the past Rule Based Expert Systems (RBES) and AI tools for decision taking in different fields (medicine, transportation engineering,...), both using algebraic inference engines and logic programming.

The key idea of this work is to develop a computer package that guides the user along a sequence of questions, in order to find out the model and/or version of the car and to detect non-original elements.

One important fact is that the available information can be incomplete (for instance, all the available information about the vehicle can be a set of photographs). Moreover, the user of the system can be sometimes unable to answer all questions, even with all the required information.

We have decided to use a hybrid approach, because:

- on one hand there are “conclusive items” that are easier to handle using rules in the style of classic RBES,
- on the other hand, when the vehicle has a mixture of characteristics from different models/versions, it is easier to compare them with the predefined ones (stored in row matrix, sequence, list format,...) in order to identify the “closest” model/version.

A computer algebra system offers all the necessary tools for implementing such an approach. The article is illustrated with a small system (implemented in the computer algebra system *Maple*, that takes advantage of its *Logic* package), devoted to the Porsche 928.

## Keywords

Expert Systems; Pattern Matching; Classic Cars; Computer Algebra Systems

# Population-based anamorphosis maps for railway radial networks

Eugenio Roanes-Lozano  
Instituto de Matemática Interdisciplinar (IMI),  
Algebra Dept., Universidad Complutense de Madrid, Spain

Alberto García-Álvarez  
Deputy Director for Renfe (Spanish Railways) Passengers Services, Spain

José Luis Galán-García  
Applied Mathematics Dept., Universidad de Málaga, Spain

Luis Mesa  
Spanish Railways Foundation, Spain

`eroanes@mat.ucm.es`

## Abstract

The Spanish railway network is radial but very complex to operate, because two different track gauges, five signalling systems and two electrification systems coexist. Therefore, how to go on developing the high speed network and which are the best routes for trains are complicated questions. We are developing, in cooperation with the Spanish Railway Foundation, software packages that can be aids to decision making in these two issues. Yet one more step in this direction is presented here.

## Keywords

Radial railway networks, Anamorphosis maps, Isochrone circle maps, Computer algebra systems

## 1 Introduction

The Spanish railway network is radial but very complex to operate, because:

- two different track gauges coexist: the so called *Iberian gauge* (1667mm) and the *international gauge* (1435mm) (used in the high speed network),
- two electrification systems have been used (3000 V DC, 25000 V AC) and, finally,
- there are different signalling systems (ASFA, ASFA 200, LZB, EBICAB, ERTMS).

The shape of the network is not due to a katabasis or anabasis of the whole Spanish society, but to the location of Madrid (the biggest city and capital) in the centre of the country and the location of the rest of big cities in the periphery. In 2013 the fares have been lowered and different discounts (for instance in low demand periods) are offered in order to attract more travelers and to increase the fraction of population using the high-speed trains.

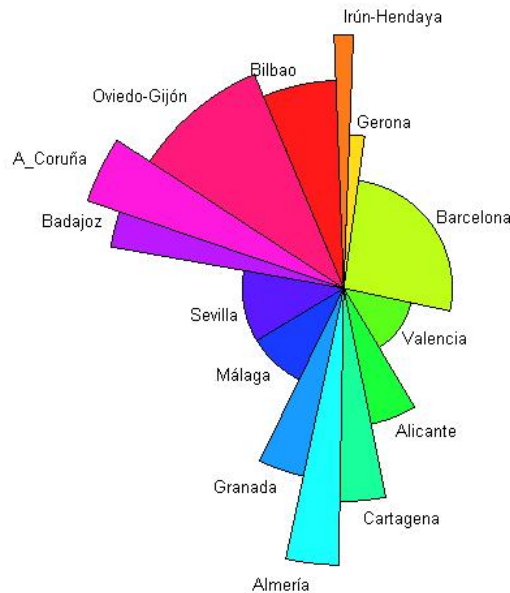
Regarding the two gauges, there are gauge changeovers at several points, so that both subnetworks are connected. A subset of the rolling stock is dual gauge. Regarding electrification and signalling systems, many locomotives and multiple units can read different signalling systems, are multi-voltage. Even hybrid rolling stock has been developed (730 series).

The high speed network has grown very quickly, and only China has nowadays a longer high speed railway network. All new lines have been built with double track and top technologies ( $\geq 300km/h$  track design, *ERTMS* traffic management system, 25000KV AC electrification, etc.).

The growth of the network has been supported by the different governments and has only been slowed down due to the economical crisis.

Nevertheless, how to go on developing the high speed network and which are the best routes for trains are complicated questions. We are developing, in cooperation with the *Spanish Railway Foundation*, software packages that can be aids to decision making in these two issues. We have followed two lines:

- We have developed (within the frame of two research projects signed between the *Spanish Railways Foundation* and the *Universidad Complutense de Madrid* and the *Universidad Politécnica de Madrid*) a computer package that is able to calculate precise timings, consumptions, costs, emissions, best routes, etc., for each piece of *Renfe*'s (main railway operator) rolling stock running on *Adif*'s (infrastructure company) lines [1].
- We have also developed what we have called *isochrone circle graphs* and a *geometric index* for radial railway networks improvement estimation [2]. *Isochrone circle graphs* were inspired by pie charts (also known as circle graphs), polar area diagrams (similar to usual pie charts, but sectors are equal angles and their area is adjusted changing their radii instead of their amplitude) and anamorphosis maps (also known as central point cartograms or distance cartograms; where the geometry of the country or region is distorted according to the time that it takes to travel to different peripheral destinations from a central origin). An *isochrone circle graph* corresponding to Spain in 2013 (centred at Madrid) can be found in the figure below.



We have followed two approaches to compute and draw *isochrone circle graphs*:

- The first approach [2] was illustrated with a sketch constructed with a Dynamic Geometry System and used sliders to change the input parameters (timing to each peripheral destination and population of these destinations). It was very comfortable to use, but the number of destinations considered was somehow fixed (changing it required to construct a complete new sketch).
- In the second approach we designed and implemented a complete new package in the CAS *Maple* that takes as input the lists of destinations, best timings and populations and builds the corresponding *isochrone circle graphs* and performs all the corresponding calculations [3]. This approach has yet another advantage: symbolic computations can be performed, and therefore parameters can be introduced in the computations.

An improved version of [3] will be presented here. It has to be emphasized that now a population-based version of an anamorphosis map can be drawn or superimposed to the *isochrone circle graph*.

## References

- [1] A. Hernando, E. Roanes–Lozano, A. García–Álvarez, L. Mesa, I. González–Franco: Optimal Route Finding and Rolling–Stock Selection for the Spanish Railways. *Comp. in Sci. & Eng.* 14/4 (2012) 82–89. DOI: <http://dx.doi.org/10.1109/MCSE.2012.80>.
- [2] E. Roanes–Lozano, A. García–Álvarez, A. Hernando: A geometric approach to the estimation of radial railway network improvement. *Rev. R. Acad. Cienc. Exactas Fís. Nat., Ser. A Mat. RACSAM* 106/1 (2012) 35–46. DOI: <http://dx.doi.org/10.1007/s13398-011-0050-6>.
- [3] E. Roanes–Lozano, A. García–Álvarez, J. L. Galán–García, L. Mesa: Estimating radial railway network improvement with a CAS. To be presented at: *FEMTEC'2013 (4th International Congress on Computational Engineering and Sciences)*, Las Vegas, May 19–24, 2013.

# An Algebraic Approach to Geometric Proof Using a Computer Algebra System

Michael Xue

Vroom Laboratory for Advanced Computing (US)

mxue@vroomlab.com

## Abstract

Geometric proof is often considered to be a challenging subject in mathematics.

The traditional approach seeks a tightly knitted sequence of statements linked together by strict logic to prove that a theorem is true. Moving from one statement to the next in traditional proofs often demands clever, if not ingenious reasoning. An algebraic approach to geometric proof, however, is more direct and algorithmic in nature. It is based on the assumption that proving a geometric theorem essentially means solving a problem in algebra. More precisely, it means solving a system of algebraic equations. An algebraic approach typically consists of the following steps:

**Step-0.** An appropriate coordinate system is chosen.

**Step-1.** The relationships between geometric elements are translated into a system of algebraic equations based on geometric data (e.g., coordinates of points, lengths and slopes of line segments, areas of figures, etc.). The expression that implies the thesis statement is identified.

**Step-2.** Solving equations in Step-1 by built-in solver in the existing Computer Algebra System (CAS). The thesis statement is then shown to be a consequence of evaluating the expression identified in Step-1 using the appropriate solution(s).

Due to the tremendous amount of calculation involved in the process, the algebraic approach becomes feasible only with the aid of CAS' powerful symbol manipulation capability. This presentation will demonstrate the algebraic approach to geometric proof by three examples using Omega, an online CAS Explorer.

### Example-1

We begin with a proof of Heron's formula concerning the area of any triangle, namely,

$$A = \sqrt{s(s-a)(s-b)(s-c)} \quad (1)$$

where  $a, b, c$  are the three sides of the triangle and  $s = \frac{a+b+c}{2}$ .

Substituting  $s$  into (1), the formula becomes

$$A = \sqrt{\frac{(a+b+c)(-a+b+c)(a-b+c)(a+b-c)}{16}} \quad (2)$$

A triangle with three known sides is shown in Fig. 1 where  $x$  is part of the base of the triangle.

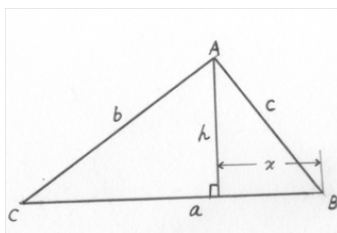


Fig. 1

By Pythagorean theorem:

$$h^2 + x^2 = c^2$$

$$h^2 + (a - x)^2 = b^2$$

To obtain  $h^2$ , we will use the following script of Omega Computer Algebra Explorer (<http://www.vroomlab.com>)

```
eq1:h^2+x^2-c^2$
eq2:h^2+(a-x)^2-b^2$
eliminate([eq1, eq2], [x, h^2])$
factor(%[1]);
```

The 'eliminate' eliminates variable  $x$  returns the value of  $h^2$ .  
The script yields

$$h^2 = \frac{(a + b + c)(-a + b + c)(a - b + c)(a + b - c)}{4a^2}.$$

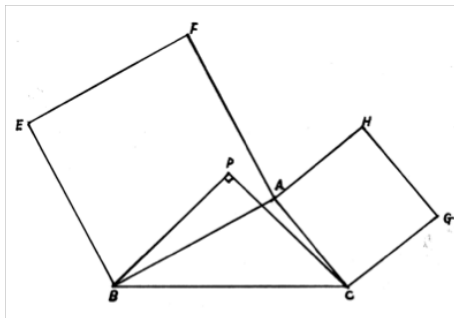
Therefore,

$$A = \frac{1}{2}ah = \sqrt{\frac{(a + b + c)(-a + b + c)(a - b + c)(a + b - c)}{16}}$$

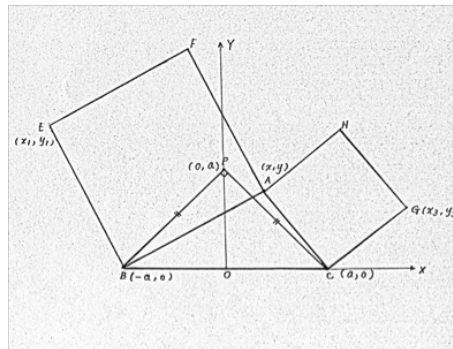
which is (2).

### Example-2

Given  $\triangle ABC$  and two squares  $ABEF$ ,  $ACGH$  in Fig. 2.(a). The squares are sitting on two sides of  $\triangle ABC$ ,  $AB$  and  $AC$ , respectively. Both squares are oriented away from the interior of  $\triangle ABC$ .  $\triangle BCP$  is an isosceles right triangle.  $P$  is on the same side of  $A$ . Prove: Points  $E$ ,  $P$  and  $G$  lie on the same line.



(a)



(b)

Fig. 2

Introducing rectangular coordinates shown in Fig. 2.(b).

From Fig. 2.(b), we observe that

$$y > 0 \tag{3}$$

$$x_1 < a \tag{4}$$

$$x_3 > a \tag{5}$$

$$CG = CA \Rightarrow (x_3 - a)^2 + y_3^2 = (x - a)^2 + y^2 \tag{6}$$

$$AB = BE \Rightarrow (x + a)^2 + y^2 = (x_1 + a)^2 + y_1^2 \tag{7}$$

$$CG \perp CA \Rightarrow y_3y = -(x - a)(x_3 - a) \tag{8}$$

$$BE \perp AB \Rightarrow y_1y = -(x_1 + a)(x + a) \tag{9}$$

Solving systems of equation (6), (7), (8), (9), we obtain four set of solutions:

$$x_1 = -y - a, y_1 = x + a, x_3 = y + a, y_3 = a - x \quad (10)$$

$$x_1 = y - a, y_1 = -x - a, x_3 = y + a, y_3 = a - x \quad (11)$$

$$x_1 = -y - a, y_1 = x + a, x_3 = a - y, y_3 = x - a \quad (12)$$

$$x_1 = y - a, y_1 = -x - a, x_3 = a - y, y_3 = x - a \quad (13)$$

Among them, only (10) truly represents the coordinates in Fig. 2.(b). The determinant

$$\frac{1}{2} \begin{vmatrix} -y - a & x + a & 1 \\ 0 & a & 1 \\ y + a & a - x & 1 \end{vmatrix}$$

is zero which implies that  $E$ ,  $P$ , and  $G$  are on the same line. See Fig. 3

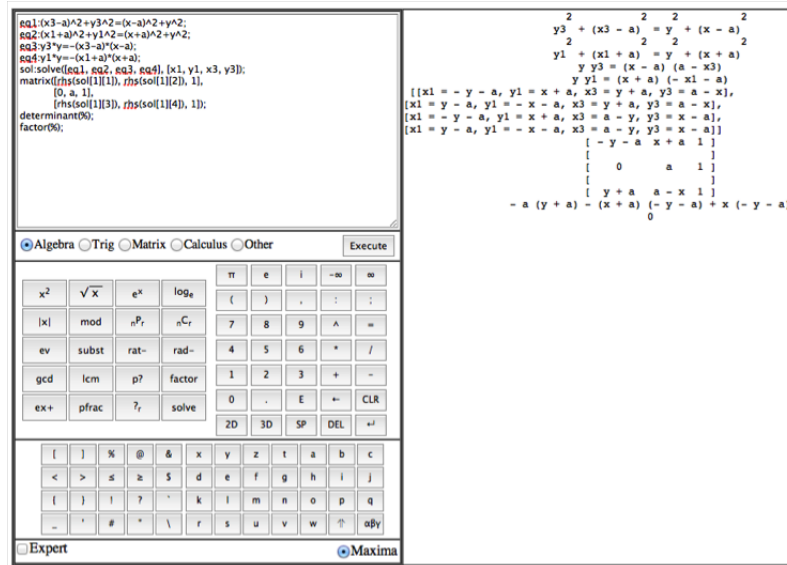


Fig. 3

The reason we do not consider (11), (12), (13) is due the fact that (11) contradicts (4) since  $y > 0, a > 0 \Rightarrow x_1 = y - a = -a + y > -a$ . By (3), (12) and (13) indicate  $x_3 = a - y < a$  which contradicts (5).

### Example-3

The area  $A$  of a triangle by three points  $(x_1, y_1), (x_2, y_2), (x_3, y_3)$  in a rectangular coordinate system can be expressed as  $|\frac{1}{2}D|$ , where  $D$  is the determinant of matrix:

$$\begin{pmatrix} x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \\ x_3 & y_3 & 1 \end{pmatrix}$$

By Heron's formula (1) in Example-1,  $A^2 = s(s - a)(s - b)(s - c)$ . Let  $B = |\frac{1}{2}D|$ ,  $B^2 = |\frac{1}{2}D|^2 = (\frac{1}{2}D)^2$ .

It is shown by Computer Algebra system that  $A^2 - B^2 = 0$  (See Fig. 4).

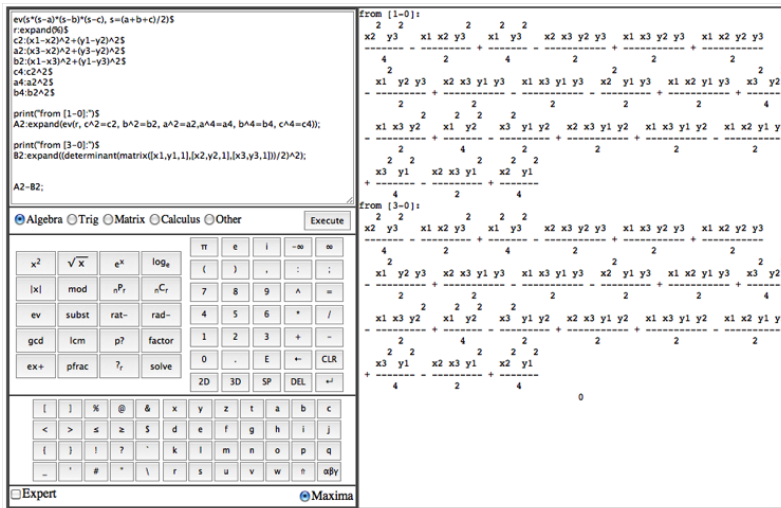


Fig. 4

$A^2 - B^2 = (A - B)(A + B) = 0$  implies that  $A = B$  since both  $A$  and  $B$  are positive quantities.



---

# Session 6: Arithmetic of Algebraic Curves

---

Organizers:

Jean-Marc Couveignes

Nicola Pagani

Tony Shaska



# Hyperbolic uniformizations through computations on ternary quadratic forms

Montserrat Alsina  
Universitat Politècnica de Catalunya BarcelonaTech

montserrat.alsina@upc.edu

## Abstract

Orders in indefinite quaternion algebras provide Fuchsian groups acting on the Poincaré half-plane, used to construct the associated Shimura curves.

We explain how, by using embedding theory, the elements of those Fuchsian groups depend on representations of integers by suitable ternary quadratic forms. Thus the explicit computation of those representations leads to explicit presentations and fundamental domains of those Fuchsian groups, the computation of CM points, and a rich interpretation of the points in the complex upper half-plane.

## Keywords

Fuchsian groups, quaternion algebras, quadratic forms, embeddings

## 1 Introduction

Let  $D, N$  be natural numbers such that  $\gcd(D, N) = 1$  and  $D$  is the product of an even number of different primes. Then there exists an indefinite quaternion algebra  $H$  over  $\mathbb{Q}$ , unique up to isomorphism, with discriminant  $D$ , given by a  $\mathbb{Q}$ -basis  $\{1, i, j, ij\}$  satisfying the relations  $i^2 = a$ ,  $j^2 = b$  and  $ij = -ji$  (plus the associative property) for some  $a, b \in \mathbb{Q}^*$ ,  $a > 0$ . As usual, we write  $H = \left(\frac{a, b}{\mathbb{Q}}\right)$ . Since  $H$  is indefinite, we can fix an embedding  $\Phi : H \hookrightarrow M(2, \mathbb{R})$ .

Let us consider an Eichler order of level  $N$ ,  $\mathcal{O}(D, N)$ , that is, a  $\mathbb{Z}$ -module of rank 4, subring of  $H$ , intersection of two maximal orders, unique up to conjugation. Basics on quaternion algebras and orders can be found at [7], [9].

Consider  $\Gamma(D, N) := \Phi(\{\alpha \in \mathcal{O}(D, N) : n(\alpha) = 1\})$ , the image of the group of units of positive norm. Then  $\Gamma(D, N) \subseteq \mathrm{SL}(2, \mathbb{R})$  is a Fuchsian group of the first kind acting on the Poincaré half-plane  $\mathcal{H} = \{x + iy \mid y > 0\}$ , and the quotient  $\Gamma(D, N) \backslash \mathcal{H}$  yields a Riemann surface. If  $D = 1$ , then  $H = M(2, \mathbb{Q})$ ,  $\Gamma(D, N) = \Gamma_0(N)$  and this construction leads to the modular curves usually denoted by  $X_0(N)$ . Otherwise, if  $D > 1$ , these Riemann surfaces are already compact and Shimura's work (cf. [8]) provides a canonical model for  $\Gamma(D, N) \backslash \mathcal{H}$  with nice properties, that will be denoted by  $X(D, N)$ , and a modular interpretation.  $X(D, N)$  are called Shimura curves associated to the subgroups  $\Gamma(D, N)$ , and they are involved in some spectacular results as the proof of Taniyama-Shimura-Weil modularity conjecture (cf. [5], [10]).

By construction, it is not so easy to make explicit these groups  $\Gamma(D, N)$  and to compute, for example, the hyperbolic uniformization of the associated Shimura curves. In particular the lack of cusps in these groups makes a big difference with the well-known modular case. Anyway, the fundamental domains of these curves allows a rich interpretation of the points in the complex upper half-plane, which can be elliptic, CM-points, etc. and even binary quadratic forms show up (cf. [3]).

The goal of this paper is to make explicit the relationship between the Fuchsian group  $\Gamma(D, N)$  and representations of integers by suitable ternary quadratic forms, in such a way that computational results on quadratic forms can be applied to this arithmetic and geometric setting.

## 2 The group of quaternion transformations via embeddings

We deal with embeddings of quadratic fields into quaternion algebras, taking into account the arithmetic of orders in both algebraic structures.

From now on consider a quadratic field  $F = \mathbb{Q}(\sqrt{d})$ , and  $\Lambda = \Lambda(d, m) \subset F$  the quadratic order of conductor  $m$ . It is well-known that  $\Lambda(d, m) = \mathbb{Z}[1, mw]$ , where  $w = \sqrt{d}$  if  $d \equiv 2, 3 \pmod{4}$ , and  $w = \frac{1+\sqrt{d}}{2}$  if  $d \equiv 1 \pmod{4}$ . For  $m = 1$ ,  $\Lambda$  is the integer ring of  $F$ .

We denote by  $\mathcal{E}(H, F)$  the set of embeddings of the quadratic field  $F$  in the quaternion algebra  $H$ . If it is non empty, we consider the restriction to the orders

$$\mathcal{E}(\mathcal{O}, \Lambda) := \{\varphi : \varphi \in \mathcal{E}(H, F), \varphi(\Lambda) \subset \mathcal{O}\}.$$

An embedding is called optimal if  $\varphi(F) \cap \mathcal{O} = \varphi(\Lambda)$ , and  $\mathcal{E}^*(\mathcal{O}, \Lambda)$  will denote the set of optimal embeddings.

The group  $\text{Nor } \mathcal{O}$  acts on  $\mathcal{E}^*(\mathcal{O}, \Lambda)$ , and we can consider the quotient  $\mathcal{E}^*(\mathcal{O}, \Lambda)/\text{Nor } \mathcal{O}$ . In the case  $\mathcal{O} = \mathcal{O}(D, N)$ , its class number can be computed following results by Eichler (cf. [1], [6]).

In our setting, those embeddings will be very interesting because, by using fundamental units in quadratic orders, they allow to compute elements in the Fuchsian group  $\Gamma(D, N)$ . They are also relevant to compute the fundamental domain of the Shimura curves  $X(D, N)$  and the corresponding tessellation of  $\mathcal{H}$ , and interesting points as elliptic and complex multiplication ones. Note that, because of the lack of cusps, a lot of information is concentrated on those points.

**Remark 2.1** *Let  $\varepsilon$  be a fundamental unit in the quadratic order  $\Lambda(d, m)$ . Put  $\xi := \varepsilon$  if  $n(\varepsilon) = 1$  and  $\xi := \varepsilon^2$  if  $n(\varepsilon) = -1$ . Then:*

$$\varphi \in \mathcal{E}(\mathcal{O}(D, N), \Lambda(d, m)) \implies \Phi(\varphi(\xi^n)) \in \Gamma(D, N), \quad \forall n \in \mathbb{Z}.$$

Conversely, every quaternion transformation can be obtained from embeddings of quadratic orders in the quaternion order as above, as it is shown in the following theorem, proved at [1].

**Theorem 2.2** *Let  $\gamma \in \Gamma(D, N)$ ,  $D > 1$ .*

*Then there exists a quadratic order  $\Lambda(d, m)$ , a number  $n \in \mathbb{Z} - \{0\}$  and an optimal embedding  $\varphi \in \mathcal{E}^*(\mathcal{O}(D, N), \Lambda(d, m))$  such that  $\Phi(\varphi(\varepsilon^n)) = \gamma$ , where  $\varepsilon$  is the fundamental unit of  $\Lambda(d, m)$ . Moreover, elliptic transformations come from imaginary quadratic fields, and hyperbolic transformations come from real quadratic fields.*

In the proof of that theorem the involved quadratic field  $\mathbb{Q}(\sqrt{d})$  is explicit: given  $\gamma \in \Gamma(D, N)$ , then  $d = \text{tr}(\gamma)^2 - 4$ .

As a consequence of the theorem, all elements in  $\Gamma(D, N)$  can be computed from the explicit computation of embeddings by using the fundamental units in quadratic fields, which can be computed algorithmically (cf. [4]). Actually it can be done by using computer algebra systems as *Magma*.

## 3 Computations via quadratic forms

Next, we shall use quadratic forms to construct those embeddings. Mainly we will use the ternary quadratic form  $n_{\mathcal{O}, 3}$ , induced by the reduced norm in a quaternion order  $\mathcal{O}$ , when we restrict to pure quaternions. To get an expression of the quadratic form, up to  $\mathbb{Z}$  equivalence, a basis of the order need to be fixed. We will use normalized basis  $\{1, v_2, v_3, v_4\}$  satisfying  $\text{tr}(v_2) = \text{tr}(v_3) = 0$ ,  $\text{tr}(v_4) \in \{0, 1\}$  (cf. [1]).

**Remark 3.1** *Consider the family of quaternion algebras of discriminant  $D = 2p$ ,  $p \equiv 3 \pmod{4}$ ,  $H_A(p) = \left(\frac{p-1}{\mathbb{Q}}\right)$ , called small ramified algebras of type A. Then a family of Eichler orders is given by  $\mathcal{O}_A(2p, N) := \mathbb{Z}[1, i, Nj, \frac{1+i+j+ij}{2}]$ ,  $N|\frac{p-1}{2}$  square-free. The corresponding ternary normic forms are:  $n_{H, 3}(Y, Z, T) = -pY^2 + Z^2 - pT^2$  and  $n_{\mathcal{O}, 3} = (1-2p)X^2 - pY^2 + N^2Z^2 + 2pXY - 2NXZ$ .*

Given a quadratic form  $f$  in  $n$  variables and  $A(f)$  the associated matrix, consider the set of integer representations of a number  $\delta$ :

$$\mathcal{R}(f, \delta; \mathbb{Z}) := \{\alpha \in \mathbb{Z}^n : f(\alpha) = \delta\} = \{\alpha \in \mathbb{Z}^n : \alpha^t A(f) \alpha = \delta\}.$$

We denote by  $\mathcal{R}^*(f, \delta; \mathbb{Z})$  those satisfying the condition  $\gcd(\alpha_1, \dots, \alpha_n) = 1$ , called primitive representations.

The following result is proved in [1] (cf. Theorem 4.26, Corollary 4.27). Note that  $n_{\mathbb{Z}+2\mathcal{O},3}$  needs to be used instead of  $n_{\mathcal{O},3}$ .

**Theorem 3.2** *Let  $\mathcal{O} \subseteq H$  an Eichler order given by a normalized basis  $\mathcal{B} = \{1, v_2, v_3, v_4\}$ . Let  $\Lambda = \Lambda(d, m) \subseteq \mathbb{Q}(\sqrt{d})$  a quadratic order of conductor  $m$  and denote  $D_\Lambda$  its discriminant. Then there is a bijective mapping*

$$\begin{aligned} \sigma : \mathcal{R}(n_{\mathbb{Z}+2\mathcal{O},3}, -D_\Lambda; \mathbb{Z}) &\longrightarrow \mathcal{E}(\mathcal{O}, \Lambda) \\ (x, y, z) &\longmapsto \varphi, \end{aligned}$$

where  $\varphi$  is the embedding defined by  $\varphi(mw) = \left( \frac{rm - z \operatorname{tr}(v_4)}{2}, x, y, z \right)_{\mathcal{B}}$ , for  $r = 0$  if  $d \equiv 2, 3 \pmod{4}$ , and  $r = 1$  if  $d \equiv 1 \pmod{4}$ . Namely,

$$\varphi(\sqrt{d}) = \begin{cases} \left( \frac{-z \operatorname{tr}(v_4)}{2m}, \frac{x}{m}, \frac{y}{m}, \frac{z}{m} \right)_{\mathcal{B}} & \text{if } d \equiv 2, 3 \pmod{4}, \\ \left( \frac{-z \operatorname{tr}(v_4)}{m}, \frac{2x}{m}, \frac{2y}{m}, \frac{2z}{m} \right)_{\mathcal{B}} & \text{if } d \equiv 1 \pmod{4}. \end{cases}$$

Moreover, primitive representations are in bijection with optimal embeddings.

**Example 3.3** *Consider a maximal order in a small ramified quaternion algebra of type A,  $\mathcal{O}_A(14, 1) = \mathbb{Z}[1, i, j, \frac{1+i+j+ij}{2}] \subseteq H_A(7) = \left( \frac{7, -1}{\mathbb{Q}} \right)$ .*

*Consider the quadratic orders  $\Lambda(-1, 1)$ ,  $\Lambda(-1, 3)$  and  $\Lambda(-1, 15)$ , in  $\mathbb{Q}(\sqrt{-1})$ . Computing representations of 1, 9 and 225 by the ternary normic form*

$$n_{\mathbb{Z}+2\mathcal{O}_A(14,1),3}(X, Y, Z) = -28X^2 + 4Y^2 - 13Z^2 - 28XZ + 4YZ,$$

we obtain the embeddings  $\varphi_s \in \mathcal{E}(H_A(7), F)$ , given by  $\varphi_s(w) = \omega_s$ ,  $1 \leq s \leq 4$ , where  $\omega_1 := j$ ,  $\omega_2 := 3i + 8j$ ,  $\omega_3 := 1/3i + 4/3j$ , and  $\omega_4 := 1/15i + 22/15j + 2/5ij$ .

Bullets in next table shows which embeddings are on each set, optimal or not.

	$\varphi_1$	$\varphi_2$	$\varphi_3$	$\varphi_4$
$\mathcal{E}(\mathcal{O}_A(7, 1), \Lambda(-1, 1))$	•	•	–	–
$\mathcal{E}^*(\mathcal{O}_A(7, 1), \Lambda(-1, 1))$	•	•	–	–
$\mathcal{E}(\mathcal{O}_A(7, 1), \Lambda(-1, 3))$	•	•	•	–
$\mathcal{E}^*(\mathcal{O}_A(7, 1), \Lambda(-1, 3))$	–	–	•	–
$\mathcal{E}(\mathcal{O}_A(7, 1), \Lambda(-1, 15))$	•	•	•	•
$\mathcal{E}^*(\mathcal{O}_A(7, 1), \Lambda(-1, 15))$	–	–	–	•

Considering the class groups of optimal embeddings and primitive representation, it is proved that the map  $\sigma$  induce a bijection between the class groups. Thus, the class number of equivalent representations can be computed too, using the classification of optimal embeddings quoted in previous section. At the example above, the integer 1 has two inequivalent representations by the ternary form  $n_{\mathbb{Z}+2\mathcal{O}_A(14,1),3}$ ; however, the integer 9 has four inequivalent ones.

As a consequence of the Theorems 2.2 and 3.2, the elements in the group  $\Gamma(D, N)$  can be found explicitly by computing representations by ternary quadratic forms.

Next, we show explicit expressions depending only on representations of integers by ternary quadratic forms the small ramified parametric case presented in Remark 3.1. They are applied to the computation of the elliptic elements in  $\Gamma(2p, N)$  and its corresponding points, and to the computation of the complex multiplication (CM) points. Both are the interesting points in this context of hyperbolic uniformization of Shimura curves in the Poincaré half-plane.

We use the explicit embedding  $\Phi : \left( \frac{p, -1}{\mathbb{Q}} \right) \hookrightarrow M(2, \mathbb{Q}(\sqrt{p})) \subset M(2, \mathbb{R})$  given by

$$\Phi(x + y\sqrt{p} + z\sqrt{-1} + t\sqrt{-p}) = \begin{pmatrix} x + y\sqrt{p} & z + t\sqrt{p} \\ -(z - t\sqrt{p}) & x - y\sqrt{p} \end{pmatrix}.$$

**Proposition 3.4** Let  $p \equiv 3 \pmod{4}$  and  $N \mid \frac{p-1}{2}$  square-free. Fix the quaternion algebra  $H_A(p)$ , the Eichler order  $\mathcal{O}_A(2p, N) = \mathbb{Z}[1, i, Nj, \frac{1+i+j+ij}{2}]$ , and the group of quaternion transformations  $\Gamma(2p, N)$  defining the Shimura curve  $X(2p, N)$ . Then:

i)  $\gamma \in \Gamma(2p, N)$  is an elliptic linear fractional transformation on  $\mathcal{H}$  of order 2 if, and only if, 
$$\gamma = \frac{1}{2} \begin{pmatrix} (2x+z)\sqrt{p} & (2Ny+z) + z\sqrt{p} \\ -(2Ny+z) + z\sqrt{p} & -(2x+z)\sqrt{p} \end{pmatrix},$$
 where  $(x, y, z) \in \mathcal{R}^*(n_{\mathbb{Z}+2\mathcal{O},3}, 4; \mathbb{Z})$ .

In this case, the corresponding elliptic point is  $\tau = \frac{(2x+z)\sqrt{p} \pm 2\iota}{-(2Ny+z) + z\sqrt{p}} \in \mathcal{H}$ .

ii) The complex points of  $X(D, N)$  with complex multiplication by a quadratic order  $\Lambda$  are

$$\left\{ \frac{(2x+z)\sqrt{p} \pm \sqrt{-D_\Lambda}\iota}{-(2Ny+z) + z\sqrt{p}} \in \mathcal{H} : (x, y, z) \in \mathcal{R}^*(n_{\mathbb{Z}+2\mathcal{O},3}, -D_\Lambda; \mathbb{Z}) \right\}.$$

We can conclude that from a fine study of the algorithms to compute representations of integers by ternary quadratic forms, new results for the complexity of computations related to the Shimura curves  $X(D, N)$  can be drawn. They would be of great interest not only in the area of Number Theory but in applications to other areas as Coding Theory or Cryptography.

## References

- [1] M. Alsina and P. Bayer, *Quaternion Orders, Quadratic Forms and Shimura Curves*, CRM Monograph Series vol. 22, AMS (2004).
- [2] M. Alsina, *Fundamental domains of the upper half plane by the action of matrix groups*, Meeting on matrix analysis and applications, Dept. Mat. Apl. I, Fac. Informática y Estadística, Univ. de Sevilla (1997), 10–17.
- [3] M. Alsina, *Binary quadratic forms and Eichler orders*, J. de Théorie des Nombres de Bordeaux **17** (2005), 13–23.
- [4] H. Cohen, *Number Theory*, Graduate Texts in Mathematics, vol. 239, Springer (2007).
- [5] G. Cornell, J. H. Silverman, and G. Stevens (eds.), *Modular forms and Fermat's last theorem*, Springer, (1997), Papers from the Instructional Conference on Number Theory and Arithmetic Geometry held at Boston University, Boston MA (1995).
- [6] A.P. Ogg, *Real points on Shimura curves*, Progress in mathematics, no. 35, Birkhäuser (1983), 277–303.
- [7] I. Reiner, *Maximal Orders*, Academic Press (1975).
- [8] G. Shimura, *Construction of class fields and zeta functions of algebraic curves*, Annals of Math. **85** (1967), 58–159.
- [9] M.F. Vigneras, *Arithmétique des algèbres de quaternions*, Lecture Notes in Math., no. 800, Springer (1980).
- [10] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Annals of Math. **141** (1995), 443–551.

# Symplectic representations for finite group actions on Riemann surfaces

Antonio Behn, Anita M. Rojas  
Universidad de Chile

Rubí Rodríguez  
Pontificia Universidad Católica de Chile

afbehn@gmail.cl

## Abstract

We present an algorithmic method to effectively compute a symplectic representation of any finite group  $G$ , coming from its action on a Riemann Surface  $M$  of some fixed genus  $g \geq 2$ . The action of the group may be specified by its signature or by the explicit group as a permutation group with generators. In particular, we find and provide a drawing of a fundamental polygon for  $M$  capturing this action of  $G$ , a symplectic basis for  $H_1(M, \mathbb{Z})$  and the action of  $G$  represented in such a basis.

In many cases we can also explicitly obtain a family of Riemann matrices of principally polarized abelian varieties of dimension  $g$ , with the action of  $G$ , describing in such a way part of the singular locus of  $\mathcal{A}_g$ . We implement this procedure over SAGE[2], and we present several examples using it.

This work has been published as “Adapted hyperbolic polygons and symplectic representations for group actions on Riemann surfaces” [1] and the SAGE routines are available online at <https://sites.google.com/a/u.uchile.cl/polygons/home>

## Keywords

symplectic representation, Riemann surface, hyperbolic polygon

## References

- [1] Antonio Behn, Rubí E. Rodríguez, and Anita M. Rojas. Adapted hyperbolic polygons and symplectic representations for group actions on Riemann surfaces. *J. Pure Appl. Algebra*, 217(3):409–426, 2013.
- [2] W.A. Stein et al. *Sage Mathematics Software (Version 5.4)*. The Sage Development Team, 2013. <http://www.sagemath.org>.

# Remarks on superelliptic curves and their Jacobians

L. Beshaj and T. Shaska  
Oakland University, Rochester, MI, USA.

beshaj@oakland.edu

## Abstract

Determining if an Abelian variety is decomposable and finding such decompositions is a problem that has been studied by many mathematicians. Methods exist in finding such decompositions for certain classes of curves; [4], [5]. In this paper we consider the superelliptic curves for genus  $g \geq 2$  and determine decompositions of them. Complete proofs are intended in [2].

## Keywords

Jacobians of curves, superelliptic curves, automorphism group

## 1 Introduction

Let  $\mathcal{X}$  be a genus  $g \geq 2$  algebraic curve defined over  $\mathbb{C}$ . We choose a symplectic homology basis for  $\mathcal{X}$ , say  $\{A_1, \dots, A_g, B_1, \dots, B_g\}$ , such that the intersection products  $A_i \cdot A_j = B_i \cdot B_j = 0$  and  $A_i \cdot B_j = \delta_{ij}$ , where  $\delta_{ij}$  is the Kronecker delta. We choose a basis  $\{w_i\}$  for the space of holomorphic 1-forms such that  $\int_{A_i} w_j = \delta_{ij}$ . The matrix  $\Omega = \left[ \int_{B_i} w_j \right]$  is the *period matrix* of  $\mathcal{X}$ . The columns of the matrix  $[I \mid \Omega]$  form a lattice  $L$  in  $\mathbb{C}^g$ . The complex torus  $\mathbb{C}^g/L$  is called the Jacobian of  $\mathcal{X}$  is denoted by  $\text{Jac}(\mathcal{X})$ .

Let  $\mathcal{H}_g$  be the *Siegel upper-half space*. Then  $\Omega \in \mathcal{H}_g$  and there is an injection

$$\mathcal{M}_g \hookrightarrow \mathcal{H}_g / Sp_{2g}(\mathbb{Z}) =: \mathcal{A}_g$$

where  $Sp_{2g}(\mathbb{Z})$  is the *symplectic group*. A non-constant morphism  $f : A \rightarrow B$  between two Abelian varieties which is surjective is called an **isogeny**. An Abelian variety is called *decomposable* if it is isogenous to a product of Abelian varieties, it is *simple* if it has non-trivial Abelian subvarieties. An Abelian variety is called **completely decomposable** if it is isogenous to a product of elliptic curves.

A map of algebraic curves  $f : \mathcal{X} \rightarrow \mathcal{Y}$  is called a **maximal covering** if it does not factor over a nontrivial isogeny. A map  $f : \mathcal{X} \rightarrow \mathcal{Y}$  induces maps between their Jacobians  $f^* : \text{Jac}(\mathcal{Y}) \rightarrow \text{Jac}(\mathcal{X})$  and  $f_* : \text{Jac}(\mathcal{X}) \rightarrow \text{Jac}(\mathcal{Y})$ . When  $f$  is maximal then  $f^*$  is injective and  $\ker(f_*)$  is connected, see [10] (p. 158) for details. Hence,  $\text{Jac}(\mathcal{X}) \cong \text{Jac}(\mathcal{Y}) \times A$ , where  $A$  is some Abelian variety.

Hence, coverings  $f : \mathcal{X} \rightarrow \mathcal{Y}$  give factors of the jacobian  $\text{Jac}(\mathcal{X})$ . Such methods have been explored for genus 2 curves in [7, 11, 12]. If the covering  $f : \mathcal{X} \rightarrow \mathcal{Y}$  is a Galois covering then its monodromy group is isomorphic to a subgroup  $H$  of the automorphism group  $G = \text{Aut}(\mathcal{X})$ . Hence a common procedure to produce decompositions of Jacobians is to explore the automorphism group of the curve.

Fix an integer  $g \geq 2$  and a finite group  $G$ . Let  $C_1, \dots, C_r$  be conjugacy classes  $\neq \{1\}$  of  $G$ . Let  $\mathbf{C} = (C_1, \dots, C_r)$ , viewed as unordered tuple, repetitions are allowed. We allow  $r$  to be zero, in which case  $\mathbf{C}$  is empty.

Consider pairs  $(X, \mu)$ , where  $X$  is a curve and  $\mu : G \rightarrow \text{Aut}(X)$  is an injective homomorphism. Mostly we will suppress  $\mu$  and just say  $X$  is a curve with  $G$ -action, or a  $G$ -curve, for short. Two  $G$ -curves  $X$  and  $X'$  are called equivalent if there is a  $G$ -equivariant isomorphism  $X \rightarrow X'$ .

We say a  $G$ -curve  $X$  is **of ramification type**  $(g, G, \mathbf{C})$  if the following holds: Firstly,  $g$  is the genus of  $X$ . Secondly, the points of the quotient  $X/G$  that are ramified in the cover  $X \rightarrow X/G$  can be labelled as  $p_1, \dots, p_r$  such that  $C_i$  is the conjugacy class in  $G$  of distinguished inertia group



generators over  $p_i$  (for  $i = 1, \dots, r$ ). (Distinguished inertia group generator means the generator that acts in the tangent space as multiplication by  $\exp(2\pi\sqrt{-1}/e)$ , where  $e$  is the ramification index). For short, we will just say  $X$  is of type  $(g, G, \mathbf{C})$ .

If  $X$  is a  $G$ -curve of type  $(g, G, \mathbf{C})$  then the genus  $g_0$  of  $X/G$  is given by the Riemann-Hurwitz formula

$$(1) \quad \frac{2(g-1)}{|G|} = 2(g_0-1) + \sum_{i=1}^r \left(1 - \frac{1}{c_i}\right)$$

where  $c_i$  is the order of the elements in  $C_i$ .

Note that  $g_0$  (the **orbit genus**) depends only on  $g$ ,  $|G|$  and the **signature**  $\mathbf{c} = (c_1, \dots, c_r)$  of the  $G$ -curve  $X$ ; see [6] for details.

Define  $\mathcal{H} = \mathcal{H}(g, G, \mathbf{C})$  to be the set of equivalence classes of  $G$ -curves of type  $(g, G, \mathbf{C})$ . By covering space theory (or the theory of Fuchsian groups),  $\mathcal{H}$  is non-empty if and only if  $G$  can be generated by elements  $\alpha_1, \beta_1, \dots, \alpha_{g_0}, \beta_{g_0}, \gamma_1, \dots, \gamma_r$  with  $\gamma_i \in C_i$  and  $\prod_j [\alpha_j, \beta_j] \prod_i \gamma_i = 1$ , where  $[\alpha, \beta] = \alpha^{-1}\beta^{-1}\alpha\beta$ .

Let  $\mathcal{M}_g$  be the moduli space of genus  $g$  curves, and  $\mathcal{M}_{g_0, r}$  the moduli space of genus  $g_0$  curves with  $r$  distinct marked points, where we view the marked points as unordered (contrary to usual procedure). Consider the map  $\Phi : \mathcal{H} \rightarrow \mathcal{M}_g$  forgetting the  $G$ -action, and the map  $\Psi : \mathcal{H} \rightarrow \mathcal{M}_{g_0, r}$  mapping (the class of) a  $G$ -curve  $X$  to the class of the quotient curve  $X/G$  together with the (unordered) set of branch points  $p_1, \dots, p_r$ . If  $\mathcal{H} \neq \emptyset$  then  $\Psi$  is surjective and has finite fibers, by covering space theory. Also  $\Phi$  has finite fibers, since the automorphism group of a curve of genus  $\geq 2$  is finite.

The set  $\mathcal{H}$  carries a structure of quasi-projective variety (over  $\mathbb{C}$ ) such that the maps  $\Phi$  and  $\Psi$  are finite morphisms. If  $\mathcal{H} \neq \emptyset$  then all components of  $\mathcal{H}$  map surjectively to  $\mathcal{M}_{g_0, r}$  (through a finite map), hence they all have the same dimension  $\delta(g, G, \mathbf{C}) := \dim \mathcal{M}_{g_0, r} = 3g_0 - 3 + r$ .

Let  $\mathcal{M}(g, G, \mathbf{C})$  denote the image of  $\Phi$ , i.e., the locus of genus  $g$  curves admitting a  $G$ -action of type  $(g, G, \mathbf{C})$ . If this locus is non-empty then each of its components has dimension  $\delta(g, G, \mathbf{C})$ . Note that  $\delta(g, G, \mathbf{C})$  depends only on  $g$ ,  $|G|$  and the signature, so we write  $\delta(g, G, \mathbf{c}) := \delta(g, G, \mathbf{C})$ .

## 2 Decomposition of Jacobians

Below we describe two methods of decomposing Jacobians using the automorphisms of curves. Both of these methods are explored in [2] to decompose Jacobians of all superelliptic curves via automorphisms.

### 2.1 Decomposing the Jacobian by group partitions

Let  $\mathcal{X}$  be a genus  $g$  algebraic curve with automorphism group  $G := \text{Aut}(\mathcal{X})$ . Let  $H \leq G$  such that  $H = H_1 \cup \dots \cup H_t$  where the subgroups  $H_i \leq H$  satisfy  $H_i \cap H_j = \{1\}$  for all  $i \neq j$ . Then,

$$\text{Jac } t^{-1}(\mathcal{X}) \times \text{Jac } |H|(\mathcal{X}/H) \cong \text{Jac } |H_1|(\mathcal{X}/H_1) \times \dots \times \text{Jac } |H_t|(\mathcal{X}/H_t)$$

The group  $H$  satisfying these conditions is called a group with partition. Elementary Abelian  $p$ -groups, the projective linear groups  $PSL_2(q)$ , Frobenius groups, dihedral groups are all groups with partition.

Let  $H_1, \dots, H_t \leq G$  be subgroups with  $H_i \cdot H_j = H_j \cdot H_i$  for all  $i, j \leq t$ , and let  $g_{ij}$  denote the genus of the quotient curve  $\mathcal{X}/(H_i \cdot H_j)$ . Then, for  $n_1, \dots, n_t \in \mathbb{Z}$  the conditions  $\sum n_i n_j g_{ij} = 0$ ,  $\sum_{j=1}^t n_j g_{ij} = 0$ , imply the isogeny relation

$$\prod_{n_i > 0} \text{Jac } n_i(\mathcal{X}/H_i) \cong \prod_{n_j < 0} \text{Jac } |n_j|(\mathcal{X}/H_j)$$

In particular, if  $g_{ij} = 0$  for  $2 \leq i < j \leq t$  and if  $g = g_{\mathcal{X}/H_2} + \dots + g_{\mathcal{X}/H_t}$ , then

$$\text{Jac }(\mathcal{X}) \cong \text{Jac }(\mathcal{X}/H_2) \times \dots \times \text{Jac }(\mathcal{X}/H_t)$$

The proof of the above statements can be found in [4]. For curves of small genus (i.e.,  $g = 2, 3, 4$ ) we can completely determine the decompositions of Jacobians based on their automorphisms. For  $g = 3$ , we have the following Theorem; see [2], [13] for details.

**Theorem 1.** Let  $\mathcal{X}$  be a genus 3 curve and  $G := \text{Aut}(\mathcal{X})$ .

a) If  $\mathcal{X}$  is hyperelliptic then

i) If  $G \cong V_4$  or  $C_2 \times C_4$ , then  $\text{Jac}(\mathcal{X}) \cong E \times \text{Jac}(\mathcal{X}_2)$ , where  $\mathcal{X}_2$  is a genus 2 curve.

ii) If  $G \cong C_2^3$  then  $\text{Jac}(\mathcal{X}) \cong E_1 \times E_2 \times E_3$

iii) If  $G \cong D_{12}, C_2 \times S_4$  or any of the groups of order 24 or 32, then  $\text{Jac}(\mathcal{X}) \cong E_1^2 \times E_2$ .

b) If  $\mathcal{X}$  is non-hyperelliptic then the following hold

i) If  $G \cong C_2$  then  $\text{Jac}(\mathcal{X}) \cong E \times \text{Jac}(\mathcal{X}_2)$  for some curves  $E$  and  $\mathcal{X}_2$ .

ii) If  $G \cong V_4$  then  $\text{Jac}(\mathcal{X}) \cong E_1 \times E_2 \times E_3$  is isogenous to the product of three elliptic curves

iii) If  $G \cong S_3, D_8$  or has order 16 or 48 then  $\text{Jac}(\mathcal{X}) \cong E_1^2 \times E_2$  for some curves  $E_1$  and  $E_2$ .

iv) If  $G \cong S_4, L_3(2)$  or  $C_2^3 \rtimes S_3$  then  $\text{Jac}(\mathcal{X}) \cong E^3$  for some elliptic curve  $E$ .

It is possible that given the equation of  $\mathcal{X}$  one can determine the equations of the elliptic or genus 2 components in all cases of the theorem as in [13] and [14].

## 2.2 Decomposing the Jacobians of curves with large groups

Given a generating system  $(0; g_1, \dots, g_r)$  for a group  $G$  we get a corresponding cover  $f : X \rightarrow \mathbb{P}^1(k)$ . From this we can construct a symplectic basis of  $H_1(X, \mathbb{Z})$  and the action of  $G$  on this basis.

Let  $W$  be a non-trivial irreducible representation of  $G$   $V$  an associated complex irreducible representation and  $s_V$  its Schur index, as denoted in [5]. There is an Abelian variety  $B_W$  and an isogeny  $\text{Jac}_W(X) \sim B_W^{\frac{\dim V}{s_V}}$ . If the subvariety  $B_W$  of  $\text{Jac}_W(X)$  is of dimension 1, then  $\text{Jac}_W(X)$  is completely decomposable. This provides another method of finding completely decomposable Jacobians. The method could work for all subgroups  $H < G$  such that  $g(X/H) = 0$ . In [5] the authors use this method to find decomposition of Jacobians for all curves  $\mathcal{X}$  which have large automorphism groups (i.e.,  $|\text{Aut}(\mathcal{X})| > 4(g-1)$ ). As we will see next, the method could be used for other groups as well. This paper focuses on superelliptic curves.

## 3 Jacobians of superelliptic curves

A curve  $\mathcal{X}$  is called superelliptic if there exist an element  $\tau \in \text{Aut}(\mathcal{X})$  such that  $\tau$  is central and  $g(\mathcal{X}/\langle \tau \rangle) = 0$ . Denote by  $K$  the function field of  $\mathcal{X}_g$  and assume that the affine equation of  $\mathcal{X}_g$  is given some polynomial in terms of  $x$  and  $y$ .

Let  $H = \langle \tau \rangle$  be a cyclic subgroup of  $G$  such that  $|H| = n$  and  $H \triangleleft G$ , where  $n \geq 2$ . Moreover, we assume that the quotient curve  $\mathcal{X}_g/H$  has genus zero. The **reduced automorphism group of  $\mathcal{X}_g$  with respect to  $H$**  is called the group  $\bar{G} := G/H$ , see [1], [8].

Assume  $k(x)$  is the genus zero subfield of  $K$  fixed by  $H$ . Hence,  $[K : k(x)] = n$ . Then, the group  $\bar{G}$  is a subgroup of the group of automorphisms of a genus zero field. Hence,  $\bar{G} < PGL_2(k)$  and  $\bar{G}$  is finite. It is a classical result that every finite subgroup of  $PGL_2(k)$  is isomorphic to one of the following:  $C_m, D_m, A_4, S_4, A_5$ .

The group  $\bar{G}$  acts on  $k(x)$  via the natural way. The fixed field of this action is a genus 0 field, say  $k(z)$ . Thus,  $z$  is a degree  $|\bar{G}| := m$  rational function in  $x$ , say  $z = \phi(x)$ . We illustrate with the following diagram:

$$\begin{array}{ccc}
 K = k(x, y) & & \mathcal{X}_g \\
 n \downarrow H & & \phi_0 \downarrow H \\
 k(x) = k(x, y^n) & & \mathbb{P}^1(k) \\
 m \downarrow \bar{G} & & \phi \downarrow \bar{G} \\
 E = k(z) & & \mathbb{P}^1(k)
 \end{array}$$

Figure 1: The automorphism groups and the corresponding covers

It obvious that  $G$  is a degree  $n$  extension of  $\bar{G}$  and  $\bar{G}$  is a finite subgroup of  $PGL_2(k)$ . Hence, if we know all the possible groups that occur as  $\bar{G}$  then we can determine  $G$  and the equation for  $K$ . The list of all groups of superelliptic curves and their equations are determined in [8] and [9]. In this paper we complete decompositions of Jacobians of superelliptic curves. Complete proofs and details are intended in [2].

**Example 1** (The Klein 4-group). If  $\mathcal{X}$  is an hyperelliptic curve and  $\bar{G} \cong C_2$  then  $G \cong V_4$ . Let  $\mathcal{X}$  be a  $V_4$ -curve. There are three elliptic involutions in  $V_4$ , say  $\tau_1, \tau_2, \tau_1\tau_2$ . Since  $\mathcal{X}$  is a superelliptic curve then one of them has to fix a genus 0 field, say  $g(\mathcal{X}/\langle\tau_1\rangle) = 0$ . Hence  $\mathcal{X}$  is hyperelliptic. Then,  $\mathcal{X}$  has equation

$$Y^2 = X^{2g+2} + a_g X^{2g} + \dots + a_1 x^2 + 1,$$

see [3]. Then  $\tau_2$  and  $\tau_1\tau_2$  fix the curves  $Y^2 = X^{g+1} + a_g X^g + \dots + a_1 X + 1$  and  $Y^2 = X(X^{g+1} + a_g X^g + \dots + a_1 X + 1)$ . Hence, the Jacobian of  $\mathcal{X}$  is the product

$$\text{Jac}(\mathcal{X}) \cong \text{Jac}(C) \times \text{Jac}(C')$$

where  $g(C) = \lfloor \frac{g-1}{2} \rfloor$  and  $g(C') = \lfloor \frac{g}{2} \rfloor$ .

In general, if  $\bar{G} \cong C_m$  then  $G \cong C_n \times C_m$  or  $G \cong C_{mn}$ . We work out details of these cases in [2]. In this work we treat in detail all the cases when  $\bar{G}$  is isomorphic to  $C_m, D_m, A_4, S_4, A_5$ . From work in [1], [8], and [9] we know all possible groups, their signatures, and the equations of the curves for all superelliptic curves. Using this data and the methods above we decompose Jacobians of all superelliptic curves.

## References

- [1] L. Beshaj, V. Hoxha, and T. Shaska, *On superelliptic curves of level  $n$  and their quotients, I*, Albanian J. Math. **5** (2011), no. 3, 115–137. MR2846162 (2012i:14036)
- [2] L. Beshaj and T. Shaska, *On superelliptic curves and their Jacobians*, (work in progress) (2013).
- [3] J. Gutierrez and T. Shaska, *Hyperelliptic curves with extra involutions*, LMS J. Comput. Math. **8** (2005), 102–115. MR2135032 (2006b:14049)
- [4] E. Kani and M. Rosen, *Idempotent relations and factors of Jacobians*, Math. Ann. **284** (1989), no. 2, 307–327. MR1000113 (90h:14057)
- [5] Herbert Lange and Anita M. Rojas, *Polarizations of isotypical components of Jacobians with group action*, Arch. Math. (Basel) **98** (2012), no. 6, 513–526. MR2935657
- [6] K. Magaard, T. Shaska, S. Shpectorov, and H. Völklein, *The locus of curves with prescribed automorphism group*, Sūrikaiseikikenkyūsho Kōkyūroku **1267** (2002), 112–141. Communications in arithmetic fundamental groups (Kyoto, 1999/2001). MR1954371
- [7] K. Magaard, T. Shaska, and H. Völklein, *Genus 2 curves that admit a degree 5 map to an elliptic curve*, Forum Math. **21** (2009), no. 3, 547–566. MR2526800 (2010h:14050)
- [8] R. Sanjeewa, *Automorphism groups of cyclic curves defined over finite fields of any characteristics*, Albanian J. Math. **3** (2009), no. 4, 131–160. MR2578064 (2011a:14045)
- [9] R. Sanjeewa and T. Shaska, *Determining equations of families of cyclic curves*, Albanian J. Math. **2** (2008), no. 3, 199–213. MR2492096 (2010d:14043)
- [10] Jean-Pierre Serre, *Groupes algébriques et corps de classes*, Publications de l’institut de mathématique de l’université de Nancago, VII. Hermann, Paris, 1959. MR0103191 (21 #1973)
- [11] T. Shaska, *Curves of genus 2 with  $(N, N)$  decomposable Jacobians*, J. Symbolic Comput. **31** (2001), no. 5, 603–617. MR1828706 (2002m:14023)
- [12] ———, *Genus 2 fields with degree 3 elliptic subfields*, Forum Math. **16** (2004), no. 2, 263–280. MR2039100 (2004m:11097)
- [13] ———, *Genus 3 hyperelliptic curves with  $(2, 4, 4)$  decomposable Jacobians*, submitted (2013).
- [14] T. Shaska and F. Thompson, *Bielliptic curves of genus 3 in the hyperelliptic moduli*, (submitted) (2013).

# ON THE AUTOMORPHISMS OF HASSETT'S MODULI SPACES

ALEX MASSARENTI

*This is an extract from a joint work with Massimiliano Mella.*

ABSTRACT. The stack  $\overline{\mathcal{M}}_{g,n}$ , parametrizing Deligne-Mumford  $n$ -pointed genus  $g$  stable curves, and its coarse moduli space  $\overline{M}_{g,n}$  have been among the most studied objects in algebraic geometry for several decades. Hassett introduced new compactifications  $\overline{\mathcal{M}}_{g,A}$  of the moduli stack  $\mathcal{M}_{g,n}$  and  $\overline{M}_{g,A}$  for the coarse moduli space  $M_{g,n}$  by assigning rational weights  $A = (a_1, \dots, a_n)$ ,  $0 < a_i \leq 1$  to the markings. In particular the classical Deligne-Mumford compactification arises for  $a_1 = \dots = a_n = 1$ . These spaces appear as intermediate steps of the blow-up construction of  $\overline{M}_{0,n}$  developed by M. Kapranov, while in higher genus may be related to the LMMP on  $\overline{M}_{g,n}$ . We deal with fibrations and automorphisms of Hassett's spaces. Our approach consists in extending some techniques already used to tackle the same kind of problems for the Deligne-Mumford compactification of  $M_{g,n}$ . As special cases we will recover known results on the automorphisms groups of  $\overline{\mathcal{M}}_{g,n}$  and  $\overline{M}_{g,n}$ . Namely  $\text{Aut}(\overline{\mathcal{M}}_{g,n}) \cong \text{Aut}(\overline{M}_{g,n}) \cong S_n$  for any  $g, n$  such that  $2g - 2 + n \geq 3$ .

## INTRODUCTION AND SURVEY ON THE AUTOMORPHISMS OF $\overline{M}_{g,n}$

The stack  $\overline{\mathcal{M}}_{g,n}$ , parametrizing Deligne-Mumford  $n$ -pointed genus  $g$  stable curves, and its coarse moduli space  $\overline{M}_{g,n}$  have been among the most studied objects in algebraic geometry for several decades.

In [Ha] B. Hassett introduced new compactifications  $\overline{\mathcal{M}}_{g,A[n]}$  of the moduli stack  $\mathcal{M}_{g,n}$  and  $\overline{M}_{g,A[n]}$  for the coarse moduli space  $M_{g,n}$ , by assigning rational weights  $A = (a_1, \dots, a_n)$ ,  $0 < a_i \leq 1$  to the markings. In genus zero some of these spaces appear as intermediate steps of the blow-up construction of  $\overline{M}_{0,n}$  developed by M. Kapranov in [Ka], while in higher genus may be related to the LMMP on  $\overline{M}_{g,n}$ .

In this paper we deal with fibrations and automorphisms of these Hassett's spaces. Our approach consists in extending some techniques introduced by A. Bruno and the authors in [BM1], [BM2] and [Ma] to study fiber type morphisms from Hassett's spaces and then apply this knowledge to compute their automorphisms groups.

The biregular automorphisms of the moduli space  $M_{g,n}$  of  $n$ -pointed genus  $g$ -stable curves and of its Deligne-Mumford compactification  $\overline{M}_{g,n}$  have been studied in a series of papers, for instance [BM2], [Ro], [GKM] and [Ma]. In [BM1] and [BM2], A. Bruno and the second author, thanks to Kapranov's works [Ka], managed to translate issues on the moduli space  $\overline{M}_{0,n}$  in terms of classical projective geometry of  $\mathbb{P}^{n-3}$ . Studying linear systems on  $\mathbb{P}^{n-3}$  with particular base loci they derived a theorem on the fibrations of  $\overline{M}_{0,n}$ .

*Date:* May 2013.

*1991 Mathematics Subject Classification.* Primary 14H10; Secondary 14D22, 14D06.

*Key words and phrases.* Moduli space of curves, pointed rational curves, fiber type morphism, automorphism.

**Theorem.** [BM2] *Let  $f : \overline{M}_{0,n} \rightarrow \overline{M}_{0,r}$  be a dominant morphism with connected fibers. Then  $f$  factors with a forgetful map.*

Via this theorem on fibrations they construct a morphism of groups between  $\text{Aut}(\overline{M}_{g,n})$  and  $S_n$ , the symmetric group on  $n$  elements, and prove the following theorem:

**Theorem.** [BM2, Theorem 3] *The automorphisms group of  $\overline{M}_{0,n}$  is isomorphic to  $S_n$  for any  $n \geq 5$ .*

As already noticed some of the Hassett's spaces are partial resolutions of Kapranov's blow-ups. The main novelty is that not all forgetful maps are well defined as morphisms. Nonetheless we are able to control this problem and derive a weighted version of the fibration theorem. This allows us to compute the automorphisms of all intermediate steps of Kapranov's construction, see Construction 1.4 for the details.

**Theorem.** *The automorphisms groups of the Hassett's spaces appearing in Construction 1.4 are given by*

- $\text{Aut}(\overline{M}_{0,A_{r,s}[n]}) \cong (\mathbb{C}^*)^{n-3} \times S_{n-2}$ , if  $r = 1$ ,  $1 < s < n - 3$ ,
- $\text{Aut}(\overline{M}_{0,A_{r,s}[n]}) \cong (\mathbb{C}^*)^{n-3} \times S_{n-2} \times S_2$ , if  $r = 1$ ,  $s = n - 3$ ,
- $\text{Aut}(\overline{M}_{0,A_{r,s}[n]}) \cong S_n$ , if  $r \geq 2$ .

In higher genus we approach the same problem. This time the fibration theorem is inherited by [GKM, Theorem 0.9], where *A. Gibney, S. Keel* and *I. Morrison* gave an explicit description of the fibrations  $\overline{M}_{g,n} \rightarrow X$  of  $\overline{M}_{g,n}$  on a projective variety  $X$  in the case  $g \geq 1$ . This theorem has been used extensively in [Ma] to construct, as in the genus zero case, morphisms of groups between  $\text{Aut}(\overline{M}_{g,n})$  and  $S_n$ , in order to prove the following theorem:

**Theorem.** [Ma, Theorem 3.9] *Let  $\overline{\mathcal{M}}_{g,n}$  be the moduli stack parametrizing Deligne-Mumford stable  $n$ -pointed genus  $g$  curves, and let  $\overline{M}_{g,n}$  be its coarse moduli space. If  $2g - 2 + n \geq 3$  then*

$$\text{Aut}(\overline{\mathcal{M}}_{g,n}) \cong \text{Aut}(\overline{M}_{g,n}) \cong S_n.$$

For  $2g - 2 + n < 3$  we have the following special behavior:

- $\text{Aut}(\overline{M}_{1,2}) \cong (\mathbb{C}^*)^2$  while  $\text{Aut}(\overline{\mathcal{M}}_{1,2})$  is trivial,
- $\text{Aut}(\overline{M}_{0,4}) \cong \text{Aut}(\overline{\mathcal{M}}_{0,4}) \cong \text{Aut}(\overline{M}_{1,1}) \cong PGL(2)$  while  $\text{Aut}(\overline{\mathcal{M}}_{1,1}) \cong \mathbb{C}^*$ ,
- $\text{Aut}(\overline{M}_g)$  and  $\text{Aut}(\overline{\mathcal{M}}_g)$  are trivial for any  $g \geq 2$ , [GKM, Corollary 0.12].

For Hassett's spaces the situation is a bit different because, in general, not all permutations of the markings define an automorphism of the space  $\overline{M}_{g,A[n]}$ . Indeed in order to define an automorphism permutations have to preserve the weight data in a suitable sense. We denote by  $\mathcal{A}_{A[n]}$  the subgroup of  $S_n$  of permutations inducing automorphisms of  $\overline{M}_{g,A[n]}$  and  $\overline{\mathcal{M}}_{g,A[n]}$ . Building on [Ma, Sections 3,4] we prove the following statement:

**Theorem.** *Let  $\overline{\mathcal{M}}_{g,A[n]}$  be the Hassett's moduli stack parametrizing weighted  $n$ -pointed genus  $g$  stable curves, and let  $\overline{M}_{g,A[n]}$  be its coarse moduli space. If  $g \geq 1$  and  $2g - 2 + n \geq 3$  then*

$$\text{Aut}(\overline{\mathcal{M}}_{g,A[n]}) \cong \text{Aut}(\overline{M}_{g,A[n]}) \cong \mathcal{A}_{A[n]}.$$

Furthermore

- $\text{Aut}(\overline{M}_{1,A[2]}) \cong (\mathbb{C}^*)^2$  while  $\text{Aut}(\overline{\mathcal{M}}_{1,A[2]})$  is trivial,
- $\text{Aut}(\overline{M}_{1,A[1]}) \cong PGL(2)$  while  $\text{Aut}(\overline{\mathcal{M}}_{1,A[1]}) \cong \mathbb{C}^*$ .

The paper is organized as follows. In the first section we recall Hassett's and Kapranov's constructions. The second section is devoted to prove the fibration theorems and in the third we compute the automorphisms groups.

### 1. HASSETT'S MODULI SPACES AND KAPRANOV'S REALIZATIONS OF $\overline{M}_{0,n}$

We work over an algebraically closed field of characteristic zero. Let  $S$  be a Noetherian scheme and  $g, n$  two non-negative integers. A family of nodal curves of genus  $g$  with  $n$  marked points over  $S$  consists of a flat proper morphism  $\pi : C \rightarrow S$  whose geometric fibers are nodal connected curves of arithmetic genus  $g$ , and sections  $s_1, \dots, s_n$  of  $\pi$ . A collection of input data  $(g, A) := (g, a_1, \dots, a_n)$  consists of an integer  $g \geq 0$  and the weight data: an element  $(a_1, \dots, a_n) \in \mathbb{Q}^n$  such that  $0 < a_i \leq 1$  for  $i = 1, \dots, n$ , and

$$2g - 2 + \sum_{i=1}^n a_i > 0.$$

**Definition 1.1.** A family of nodal curves with marked points  $\pi : (C, s_1, \dots, s_n) \rightarrow S$  is stable of type  $(g, A)$  if

- the sections  $s_1, \dots, s_n$  lie in the smooth locus of  $\pi$ , and for any subset  $\{s_{i_1}, \dots, s_{i_r}\}$  with non-empty intersection we have  $a_{i_1} + \dots + a_{i_r} \leq 1$ ,
- $K_\pi + \sum_{i=1}^n a_i s_i$  is  $\pi$ -relatively ample.

*B. Hassett* in [Ha, Theorem 2.1] proved that given a collection  $(g, A)$  of input data, there exists a connected Deligne-Mumford stack  $\overline{\mathcal{M}}_{g,A[n]}$ , smooth and proper over  $\mathbb{Z}$ , representing the moduli problem of pointed stable curves of type  $(g, A)$ . The corresponding coarse moduli scheme  $\overline{M}_{g,A[n]}$  is projective over  $\mathbb{Z}$ .

Furthermore by [Ha, Theorem 3.8] a weighted pointed stable curve admits no infinitesimal automorphisms and its infinitesimal deformation space is unobstructed of dimension  $3g - 3 + n$ . Then  $\overline{\mathcal{M}}_{g,A[n]}$  is a smooth Deligne-Mumford stack of dimension  $3g - 3 + n$ .

**Remark 1.2.** Since  $\overline{\mathcal{M}}_{g,A[n]}$  is smooth as a Deligne-Mumford stack the coarse moduli space  $\overline{M}_{g,A[n]}$  has finite quotient singularities, that is étale locally it is isomorphic to a quotient of a smooth scheme by a finite group. In particular  $\overline{M}_{g,A[n]}$  is normal.

Fixed  $g, n$ , consider two collections of weight data  $A[n], B[n]$  such that  $a_i \geq b_i$  for any  $i = 1, \dots, n$ . Then there exists a birational *reduction morphism*

$$\rho_{B[n],A[n]} : \overline{\mathcal{M}}_{g,A[n]} \rightarrow \overline{\mathcal{M}}_{g,B[n]}$$

associating to a curve  $[C, s_1, \dots, s_n] \in \overline{\mathcal{M}}_{g,A[n]}$  the curve  $\rho_{B[n],A[n]}([C, s_1, \dots, s_n])$  obtained by collapsing components of  $C$  along which  $K_C + b_1 s_1 + \dots + b_n s_n$  fails to be ample.

Furthermore, for any  $g$  consider a collection of weight data  $A[n] = (a_1, \dots, a_n)$  and a subset  $A[r] := (a_{i_1}, \dots, a_{i_r}) \subset A$  such that  $2g - 2 + a_{i_1} + \dots + a_{i_r} > 0$ . Then there exists a *forgetful morphism*

$$\pi_{A[n],A[r]} : \overline{\mathcal{M}}_{g,A[n]} \rightarrow \overline{\mathcal{M}}_{g,A[r]}$$

associating to a curve  $[C, s_1, \dots, s_n] \in \overline{\mathcal{M}}_{g,A[n]}$  the curve  $\pi_{A[n],A[r]}([C, s_1, \dots, s_n])$  obtained by collapsing components of  $C$  along which  $K_C + a_{i_1} s_{i_1} + \dots + a_{i_r} s_{i_r}$  fails to be ample.

For the details see [Ha, Section 4].

In the following we will be especially interested in the boundary of  $\overline{M}_{g,A[n]}$ . The boundary of  $\overline{M}_{g,A[n]}$ , as for  $\overline{M}_{g,n}$ , has a stratification whose loci, called strata, parametrize curves of a certain topological type and with a fixed configuration of the marked points.

We denote by  $\Delta_{irr}$  the locus in  $\overline{M}_{g,A[n]}$  parametrizing irreducible nodal curves with  $n$  marked points, and by  $\Delta_{i,P}$  the locus of curves with a node which divides the curve into a component of genus  $i$  containing the points indexed by  $P$  and a component of genus  $g - i$  containing the remaining points.

*Kapranov's blow-up constructions.* We follow [Ka]. Let  $(C, x_1, \dots, x_n)$  be a genus zero  $n$ -pointed stable curve. The dualizing sheaf  $\omega_C$  of  $C$  is invertible, see [Kn]. By [Kn, Corollaries 1.10 and 1.11] the sheaf  $\omega_C(x_1 + \dots + x_n)$  is very ample and has  $n - 1$  independent sections. Then it defines an embedding  $\varphi : C \rightarrow \mathbb{P}^{n-2}$ . In particular if  $C \cong \mathbb{P}^1$  then  $\deg(\omega_C(x_1 + \dots + x_n)) = n - 2$ ,  $\omega_C(x_1 + \dots + x_n) \cong \varphi^* \mathcal{O}_{\mathbb{P}^{n-2}}(1) \cong \mathcal{O}_{\mathbb{P}^1}(n - 2)$ , and  $\varphi(C)$  is a degree  $n - 2$  rational normal curve in  $\mathbb{P}^{n-2}$ . By [Ka, Lemma 1.4] if  $(C, x_1, \dots, x_n)$  is stable the points  $p_i = \varphi(x_i)$  are in linear general position in  $\mathbb{P}^{n-2}$ .

This fact combined with a careful analysis of limits in  $\overline{M}_{0,n}$  of 1-parameter families in  $M_{0,n}$  led M. Kapranov to prove the following theorem:

**Theorem 1.3.** [Ka, Theorem 0.1] *Let  $p_1, \dots, p_n \in \mathbb{P}^{n-2}$  be  $n$  points in linear general position, and let  $V_0(p_1, \dots, p_n)$  be the scheme parametrizing rational normal curves through  $p_1, \dots, p_n$ . Consider  $V_0(p_1, \dots, p_n)$  as a subscheme of the Hilbert scheme  $\mathcal{H}$  parametrizing subschemes of  $\mathbb{P}^{n-2}$ . Then*

- $V_0(p_1, \dots, p_n) \cong M_{0,n}$ .
- Let  $V(p_1, \dots, p_n)$  be the closure of  $V_0(p_1, \dots, p_n)$  in  $\mathcal{H}$ . Then  $V(p_1, \dots, p_n) \cong \overline{M}_{0,n}$ .

Kapranov's construction allows to translate many issues of  $\overline{M}_{0,n}$  into statements on linear systems on  $\mathbb{P}^{n-3}$ . Consider a general line  $L_i \subset \mathbb{P}^{n-2}$  through  $p_i$ . There is a unique rational normal curve  $C_{L_i}$  through  $p_1, \dots, p_n$  and with tangent direction  $L_i$  in  $p_i$ . Let  $[C, x_1, \dots, x_n] \in \overline{M}_{0,n}$  be a stable curve and let  $\Gamma \in V_0(p_1, \dots, p_n)$  be the corresponding curve. Since  $p_i \in \Gamma$  is a smooth point considering the tangent line  $T_{p_i}\Gamma$ , with some work [Ka], we get a morphism

$$f_i : \overline{M}_{0,n} \rightarrow \mathbb{P}^{n-3}, [C, x_1, \dots, x_n] \mapsto T_{p_i}\Gamma.$$

Furthermore  $f_i$  is birational and it defines an isomorphism on  $M_{0,n}$ . The birational maps  $f_j \circ f_i^{-1}$

$$\begin{array}{ccc} & \overline{M}_{0,n} & \\ f_i \swarrow & & \searrow f_j \\ \mathbb{P}^{n-3} & \xrightarrow{f_j \circ f_i^{-1}} & \mathbb{P}^{n-3} \end{array}$$

are standard Cremona transformations of  $\mathbb{P}^{n-3}$  [Ka, Proposition 2.12]. For any  $i = 1, \dots, n$  the class  $\Psi_i$  is the line bundle on  $\overline{M}_{0,n}$  whose fiber on  $[C, x_1, \dots, x_n]$  is the tangent line  $T_{p_i}C$ . From the previous description we see that the line bundle  $\Psi_i$  induces the birational morphism  $f_i : \overline{M}_{0,n} \rightarrow \mathbb{P}^{n-3}$ , that is  $\Psi_i = f_i^* \mathcal{O}_{\mathbb{P}^{n-3}}(1)$ . In [Ka] Kapranov proved that  $\Psi_i$  is big and globally generated, and that the birational morphism  $f_i$  is an iterated blow-up of the projections from  $p_i$  of the points  $p_1, \dots, \hat{p}_i, \dots, p_n$  and of all strict transforms of the linear spaces they generate, in order of increasing dimension.

**Construction 1.4.** [Ka] More precisely, fixed  $(n-1)$ -points  $p_1, \dots, p_{n-1} \in \mathbb{P}^{n-3}$  in linear general position:

- (1) Blow-up the points  $p_1, \dots, p_{n-2}$ , then the lines  $\langle p_i, p_j \rangle$  for  $i, j = 1, \dots, n-2, \dots$ , the  $(n-5)$ -planes spanned by  $n-4$  of these points.
- (2) Blow-up  $p_{n-1}$ , the lines spanned by pairs of points including  $p_{n-1}$  but not  $p_{n-2}, \dots$ , the  $(n-5)$ -planes spanned by  $n-4$  of these points including  $p_{n-1}$  but not  $p_{n-2}$ .
- $\vdots$
- ( $r$ ) Blow-up the linear spaces spanned by subsets  $\{p_{n-1}, p_{n-2}, \dots, p_{n-r+1}\}$  so that the order of the blow-ups is compatible by the partial order on the subsets given by inclusion, the  $(r-1)$ -planes spanned by  $r$  of these points including  $p_{n-1}, p_{n-2}, \dots, p_{n-r+1}$  but not  $p_{n-r}, \dots$ , the  $(n-5)$ -planes spanned by  $n-4$  of these points including  $p_{n-1}, p_{n-2}, \dots, p_{n-r+1}$  but not  $p_{n-r}$ .
- $\vdots$

( $n-3$ ) Blow-up the linear spaces spanned by subsets  $\{p_{n-1}, p_{n-2}, \dots, p_4\}$ .

The composition of these blow-ups is the morphism  $f_n : \overline{M}_{0,n} \rightarrow \mathbb{P}^{n-3}$  induced by the psi-class  $\Psi_n$ . Identifying  $\overline{M}_{0,n}$  with  $V(p_1, \dots, p_n)$ , and fixing a general  $(n-3)$ -plane  $H \subset \mathbb{P}^{n-2}$ , the morphism  $f_n$  associates to a curve  $C \in V(p_1, \dots, p_n)$  the point  $T_{p_n}C \cap H$ .

We denote by  $W_{r,s}[n]$  the variety obtained at the  $r$ -th step once we finish blowing-up the subspaces spanned by subsets  $S$  with  $|S| \leq s+r-2$ , and by  $W_r[n]$  the variety produced at the  $r$ -th step. In particular  $W_{1,1}[n] = \mathbb{P}^{n-3}$  and  $W_{n-3}[n] = \overline{M}_{0,n}$ .

In [Ha, Section 6.1] Hassett interprets the intermediate steps of Construction 1.4 as moduli spaces of weighted rational curves. Consider the weight data

$$A_{r,s}[n] := \underbrace{(1/(n-r-1), \dots, 1/(n-r-1))}_{(n-r-1) \text{ times}}, s/(n-r-1), \underbrace{1, \dots, 1}_{r \text{ times}}$$

for  $r = 1, \dots, n-3$  and  $s = 1, \dots, n-r-2$ . Then  $W_{r,s}[n] \cong \overline{M}_{0,A_{r,s}[n]}$ , and the Kapranov's map  $f_n : \overline{M}_{0,n} \rightarrow \mathbb{P}^{n-3}$  factorizes as a composition of reduction morphisms

$$\begin{aligned} \rho_{A_{r,s-1}[n], A_{r,s}[n]} : \overline{M}_{0,A_{r,s}[n]} &\rightarrow \overline{M}_{0,A_{r,s-1}[n]}, \quad s = 2, \dots, n-r-2, \\ \rho_{A_{r,n-r-2}[n], A_{r+1,1}[n]} : \overline{M}_{0,A_{r+1,1}[n]} &\rightarrow \overline{M}_{0,A_{r,n-r-2}[n]}. \end{aligned}$$

**Remark 1.5.** The Hassett's space  $\overline{M}_{A_{1,n-3}[n]}$ , that is  $\mathbb{P}^{n-3}$  blown-up at all the linear spaces of codimension at least two spanned by subsets of  $n-2$  points in linear general position, is the Losev-Manin's moduli space  $\overline{L}_{n-2}$  introduced by *A. Losev* and *Y. Manin* in [LM], see [Ha, Section 6.4]. The space  $\overline{L}_{n-2}$  parametrizes  $(n-2)$ -pointed chains of projective lines  $(C, x_0, x_\infty, x_1, \dots, x_{n-2})$  where:

- $C$  is a chain of smooth rational curves with two fixed points  $x_0, x_\infty$  on the extremal components,
- $x_1, \dots, x_{n-2}$  are smooth marked points different from  $x_0, x_\infty$  but non necessarily distinct,
- there is at least one marked point on each component.

By [LM, Theorem 2.2] there exists a smooth, separated, irreducible, proper scheme representing this moduli problem. Note that after the choice of two marked points in  $\overline{M}_{0,n}$  playing the role of  $x_0, x_\infty$  we get a birational morphism  $\overline{M}_{0,n} \rightarrow \overline{L}_{n-2}$  which is nothing



but a reduction morphism.

For example  $\overline{L}_1$  is a point parametrizing a  $\mathbb{P}^1$  with two fixed points and a free point,  $\overline{L}_2 \cong \mathbb{P}^1$ , and  $\overline{L}_3$  is  $\mathbb{P}^2$  blown-up at three points in general position, that is a Del Pezzo surface of degree six, see [Ha, Section 6.4] for further generalizations.

#### REFERENCES

- [BM1] A. BRUNO, M. MELLA, *On some fibrations of  $\overline{M}_{0,n}$* , arXiv:1105.3293v1 [math.AG].
- [BM2] A. BRUNO, M. MELLA, *The automorphisms group of  $\overline{M}_{0,n}$* , J. Eur. Math. Soc. Volume 15, Issue 3, 2013, pp. 949-968.
- [DI] I. V. DOLGACHEV, V. A. ISKOVSKIKH, *Finite subgroups of the plane Cremona group*, Algebra, arithmetic, and geometry: in honor of Yu. I. Manin. Vol. I, 443-548, Progr. Math., 269, Birkhäuser Boston, Inc., Boston, MA, 2009.
- [FMN] B. FANTECHI, E. MANN, F. NIRONI, *Smooth toric DM stacks*, J. Reine Angew. Math. 648 (2010), 201-244.
- [GKM] A. GIBNEY, S. KEEL, I. MORRISON, *Towards the ample cone of  $\overline{M}_{g,n}$* , J. Amer. Math. Soc. 15 (2002), 273-294.
- [Ha] B. HASSETT, *Moduli spaces of weighted pointed stable curves*, Advances in Mathematics 173 (2003), Issue 2, 316-352.
- [Ka] M. KAPRANOV, *Veronese curves and Grothendieck-Knudsen moduli spaces  $\overline{M}_{0,n}$* , Jour. Alg. Geom. 2 (1993), 239-262.
- [Kn] F. KNUDSEN, *The projectivity of the moduli space of stable curves II: the stack  $M_{g,n}$* , Math. Scand. 52 (1983), 161-199.
- [LM] A. LOSEV, Y. MANIN, *New moduli spaces of pointed curves and pencils of flat connections*, Michigan Math. J. Volume 48, Issue 1 (2000), 443-472.
- [Ma] A. MASSARENTI, *The Automorphisms group of  $\overline{M}_{g,n}$* , arXiv:1110.1464v1 [math.AG].
- [Mok] S. MOCHIZUKI, *Correspondences on hyperbolic curves*, J. Pure Applied Algebra, 131 (1998), 227-244.
- [Ro] H.L. ROYDEN, *Automorphisms and isometries of Teichmüller spaces*, Advances in the theory of Riemann surfaces Ed. by L. V. Ahlfors, L. Bers, H. M. Farkas, R. C. Gunning, I. Kra, H. E. Rauch, Annals of Math. Studies No.66 (1971), 369-383.

ALEX MASSARENTI, SISSA, VIA BONOMEA 265, 34136 TRIESTE, ITALY  
*E-mail address:* alex.massarenti@sissa.it

# From relations in the moduli spaces of curves, to recursions in Gromov-Witten theory

Nicola Pagani

## Abstract

As discovered by Kontsevich in the ninties, each relation in the cohomology of the moduli space of curves gives rise to recursions for enumerative problems, through Gromov-Witten theory. In this talk, I will focus on a new genus 2 relation and on its consequences. The main idea is the following. In low genus and with few marked points, one can write down all additive generators of the cohomology of the moduli space of stable,  $n$ -pointed curves of genus  $g$ , and then intersect all dimension  $k$  classes with all codimension  $k$  classes, and look for the kernel of the resulting matrix. As Poincaré duality holds for the moduli space of stable curves, such kernel consists of relations among cohomology classes. With this idea, and building on previous results of Bergström and Tavakol, we find a new relation in  $\overline{\mathcal{M}}_{2,6}$ . I will try to emphasize the computer-assisted and algorithmic aspects involved in this work.

## Keywords

moduli spaces, tautological ring, Gromov-Witten

# On the Approximate Parametrization Problem of Algebraic Curves

S.L. Rueda,

Dpto. de Matemática Aplicada

E.T.S. Arquitectura, Universidad Politécnica de Madrid

E-28040 Madrid, Spain

J. Sendra

Dpto. Matemática Aplicada I.T. Telecomunicación. UPM, Spain

Research Center on Software Technologies

and Multimedia Systems for Sustainability (CITSEM)

J.R. Sendra

Dpto. de Física y Matemáticas, Universidad de Alcalá

E-28871 Madrid, Spain

sonialuisa.rueda@upm.es, jsendra@euitt.upm.es, rafael.sendra@uah.es

## Abstract

The problem of parametrizing approximately algebraic curves and surfaces is an active research field, with many implications in practical applications. The problem can be treated locally or globally. We formally state the problem, in its global version for the case of algebraic curves (planar or spatial), and we report on some algorithms approaching it, as well as on the associated error distance analysis.

## Keywords

Rational Curve, Approximate Parametrization, Hausdorff distance

## 1 Introduction

Let us say that, within the development of some algebraic computation, probably coming from an applied problem in geometric modeling or in computer aided geometric design, as for instance the intersection of two implicitly given algebraic surfaces, we get an algebraic (planar or spatial) curve  $\mathcal{D}$  that, because of the nature of the problem we are treating, is expected to be rational. However, because of imprecisions (e.g. in the input data or in the arithmetic used in the process), the curve  $\mathcal{D}$  has positive genus, and hence cannot be parametrized with rational functions. The approximate parametrization problem asks for the computation of an algebraic curve  $\overline{\mathcal{D}}$  of genus zero, being in the vicinity of  $\mathcal{D}$ , as well as a rational parametrization of the curve  $\overline{\mathcal{D}}$ ; since we are dealing with sets, the distance (i.e. the vicinity) between  $\mathcal{D}$  and  $\overline{\mathcal{D}}$  is measured using the Hausdorff distance associated to the usual Euclidean distance in  $\mathbb{R}^2$  or  $\mathbb{R}^3$ ; see [1]. We report here on the main ideas developed in [6],[7], [9]. Additional work for this problem can be found in [8], [10], [11]; for the local treatment of the problem, one may check [3], [2], [4], [5].

In the following, we focus on the planar case treatment, developed in [6]. For the space case treatment, we refer to [9]. For this purpose we needed to introduce some new concepts as  $\epsilon$ -points,  $\epsilon$ -genus, etc, where  $\epsilon > 0$  is given. Intuitively speaking, the  $\epsilon$ -singularities are points that, although not singular, are *almost* singular. Additionally, we introduce the notion of  $\epsilon$ -multiplicity. The main difficulty that appears is that, in general, one has more  $\epsilon$ -points than expected. To overtake this difficulty we pass, via an equivalence relation, from the  $\epsilon$ -locus (that is, the union of the  $\epsilon$ -singularities and the exact singularities) to a quotient set with finitely many equivalence classes that we call clusters. These clusters play now the role of the classical singularities. We distinguish two types of clusters: those containing exact non-ordinary singularities and the others. To each cluster we associate a representative and a multiplicity as follows:

- If the cluster contains, at least, one exact non-ordinary singularity we assign as multiplicity the maximum exact multiplicity that the non-ordinary singularities provide through their blowing up, and as representative a non-ordinary singularity in the cluster for which the maximum is achieved the maximum; we store the tuple of singularities generated through the blowing up of the representative.
- If the cluster does not contain exact non-ordinary singularities, we assign as multiplicity the maximum of the  $\epsilon$ -multiplicities of their elements, and as representative an element of the cluster where maximum is achieved.

**Notation.** We use the following terminology.  $\|\cdot\|$  and  $\|\cdot\|_2$  denote the polynomial  $\infty$ -norm and the usual unitary norm in  $\mathbb{C}^2$ , respectively.  $|\cdot|$  denotes the module in the field  $\mathbb{C}$  of complex numbers. The partial derivatives of a polynomial  $g \in \mathbb{C}[x, y]$  are denoted by  $g^{\vec{v}} := \frac{\partial^{i+j} g}{\partial^i x \partial^j y}$  where  $\vec{v} = (i, j) \in \mathbb{N}^2$ ; we assume that  $g^{\vec{0}} = g$ . Moreover, for  $\vec{v} = (i, j) \in \mathbb{N}^2$ ,  $|\vec{v}|_* = i + j$ . Also,  $\vec{e}_1 = (1, 0)$  and  $\vec{e}_2 = (0, 1)$ . In addition, let  $\mathcal{D} \subset \mathbb{C}^2$  be an irreducible plane curve over  $\mathbb{C}$ , and let  $f(x, y)$  be its defining polynomial. Furthermore, let  $\epsilon \in \mathbb{R}$  be such that  $0 < \epsilon < 1$ .

## 2 $\epsilon$ -points

The basic ingredient of our reasoning is the notion of  $\epsilon$ -point; the concept of  $\epsilon$ -point of an algebraic variety was introduced by the authors (see [6], [7], [8]) as a generalization of the notion of approximate root of a univariate polynomial. Let  $P \in \mathbb{C}^2$ , we say that  $P$  is an  $\epsilon$ -(affine) point of  $\mathcal{D}$  if  $|f(P)| < \epsilon\|f\|$ . Moreover, if  $P$  is an  $\epsilon$ -point of  $\mathcal{D}$ , we define the  $\epsilon$ -multiplicity of  $P$  on  $\mathcal{D}$  (we denote it by  $\text{mult}_\epsilon(P, \mathcal{D})$ ) as the smallest natural number  $r \in \mathbb{N}$  satisfying that

- (1)  $\forall \vec{v} \in \mathbb{N}^2$ , such that  $0 \leq |\vec{v}|_* \leq r - 1$ , it holds that  $|f^{\vec{v}}(P)| < \epsilon\|f\|$ ,
- (2)  $\exists \vec{v} \in \mathbb{N}^2$ , with  $|\vec{v}|_* = r$ , such that  $|f^{\vec{v}}(P)| \geq \epsilon\|f\|$ .

In this situation, we say that  $P$  is an  $\epsilon$ -(affine) simple point of  $\mathcal{D}$  if  $\text{mult}_\epsilon(P, \mathcal{D}) = 1$ ; otherwise,  $P$  is an  $\epsilon$ -(affine) singularity of  $\mathcal{D}$ . Furthermore, we say that  $P$  is a  $k$ -pure  $\epsilon$ -singularity of  $\mathcal{D}$ , with  $k \in \{1, 2\}$ , if  $\text{mult}_\epsilon(P, \mathcal{D}) > 1$  and  $|f^{\text{mult}_\epsilon(P, \mathcal{D}) \cdot \vec{e}_k}(P)| \geq \epsilon\|f\|$ . In addition, we say that  $P$  is an  $\epsilon$ -(affine) ramification point of  $\mathcal{D}$  if  $\text{mult}_\epsilon(P, \mathcal{D}) = 1$ , and either  $|f^{\vec{e}_1}(P)| < \epsilon\|f\|$  or  $|f^{\vec{e}_2}(P)| < \epsilon\|f\|$ .

Finally, we introduce the weight of an  $\epsilon$ -singularity. This will be used for defining the  $\epsilon$ -genus. Let  $P$  be an  $\epsilon$ -singularity of  $\mathcal{D}$  and  $r = \text{mult}_\epsilon(P, \mathcal{D})$ . If  $P$  is  $k$ -pure, with  $k \in \{1, 2\}$ , we define the  $k$ -weight of  $P$  as

$$\text{weight}_k(P) = \max_{i=0, \dots, r-1} \left\{ \left| \frac{r! \cdot f^{i \cdot \vec{e}_k}(P)}{i! \cdot f^{r \cdot \vec{e}_k}(P)} \right|^{\frac{1}{r-i}} \right\}.$$

If  $P$  is pure in both directions, we define **weight** of  $P$ , as  $\text{weight}(P) = \max\{\text{weight}_1(P), \text{weight}_2(P)\}$  and as the corresponding  $k$ -weight otherwise.

## 3 $\epsilon$ -rationality

Once we have defined the  $\epsilon$ -singularities and their  $\epsilon$ -multiplicities, we introduce the notion of  $\epsilon$ -genus. This seems easy, since the genus can be introduced by means of multiplicities and we already have the notion of  $\epsilon$ -multiplicity. However, the main problem is that there are more  $\epsilon$ -singularities than expected. To face this problem, we introduce an equivalence relation over the set of  $\epsilon$ -singularities and the equivalence classes would play the role of the  $\epsilon$ -singularities in the  $\epsilon$ -genus formula. More precisely, let  $\mathcal{S}$  be a finite set of  $\epsilon$ -singularities of  $\mathcal{D}$ . In addition, let  $\mathcal{N}$  be the finite set (maybe empty) of exact non-ordinary singularities of  $\mathcal{D}$ . We replace  $\mathcal{S}$  by  $\mathcal{S} \cup \mathcal{N}$ . Also, for  $P \in \mathcal{N}$  we will refer to the **tuple of neighboring multiplicities** of  $P$ , and we will denote it by  $\text{NeighMult}(P)$ , as the tuple of all exact multiplicities of  $P$  and the neighboring points generated through its blowing up. For  $P \in \mathcal{S}$  we define the **radius** of  $P$ , and we denote it by  $\text{radius}(P)$ , as

$$\text{radius}(P) = \begin{cases} \mathcal{R}_{\text{out}}(\text{weight}(P)) & \text{if } P \text{ is pure} \\ 0 & \text{otherwise} \end{cases}$$

where  $\mathcal{R}_{\text{out}}$  is Sasaki-Terui out rational function, namely,

$$\mathcal{R}_{\text{out}}(x) = \frac{1}{2} - \frac{x(1-9x)}{2(1+3x)} - \frac{32x^2}{(1+3x)^3}.$$

Now, we introduce the following equivalence relation in  $\mathcal{S}$ . Let  $P, Q \in \mathcal{S}$ , then

$$P \mathcal{R} Q \iff \begin{cases} P \mathcal{R}^* Q \\ \text{or there exist } P_1, \dots, P_n \in \mathcal{S} \text{ such that } P \mathcal{R}^* P_1, \dots, P_n \mathcal{R}^* Q \end{cases}$$

where

$$P \mathcal{R}^* Q \iff \|P - Q\|_2 + |\text{radius}(P) - \text{radius}(Q)| < \mathcal{R}_{\text{out}}(\epsilon).$$

We define the ( $\epsilon$ -singular) clusters of  $\mathcal{D}$  as the equivalence classes in  $\mathcal{S}/\mathcal{R}$ . In addition, we distinguish two type of clusters: those whose intersection with  $\mathcal{N}$  is empty and the others. Let  $\mathfrak{C}^{\text{ord}}$  be the set of all clusters of the first type, and let  $\mathfrak{C}^{\text{non}}$  be the set of all clusters of the second type. So,  $\mathcal{S}/\mathcal{R}$  decomposes as

$$\mathcal{S}/\mathcal{R} = \mathfrak{C}^{\text{ord}} \cup \mathfrak{C}^{\text{non}}.$$

In this situation, if  $\mathfrak{C}^{\text{ord}} = \{\mathcal{C}luster_{r_i}(P_i)\}_{i=1, \dots, s_1}$  and  $\mathfrak{C}^{\text{non}} = \{\mathcal{C}luster_{T_i}(M_i)\}_{i=1, \dots, s_2}$ , with  $T_i = (k_{i,1}, \dots, k_{i,\ell_i})$ , we define the  $\epsilon$ -genus of  $\mathcal{D}$  as

$$\epsilon\text{-genus}(\mathcal{D}) = \frac{(\deg(\mathcal{D}) - 1)(\deg(\mathcal{D}) - 2)}{2} - \sum_{i=1}^{s_1} \frac{r_i(r_i - 1)}{2} - \sum_{i=1}^{s_2} \sum_{j=1}^{\ell_i} \frac{k_{i,j}(k_{i,j} - 1)}{2}.$$

In addition, we say that  $\mathcal{D}$  is  $\epsilon$ -rational if  $\epsilon\text{-genus}(\mathcal{D}) = 0$ .

In [6], for the application of the planar approximate parametrization algorithm, we imposed among other conditions that  $\mathcal{D}$  has proper degree and that  $\mathcal{D}$  is  $\epsilon$ -irreducible over  $\mathbb{C}$ . These two notions depend on  $\epsilon$ . More precisely,  $\mathcal{D}$  has proper degree  $d > 0$  if the total degree of  $f$  is  $\ell$ , and  $\exists \vec{v} \in \mathbb{N}^2$ , with  $|\vec{v}|_* = \ell$ , such that  $|f^{\vec{v}}| > \epsilon \|f\|$ . Moreover, we say that  $\mathcal{D}$  is  $\epsilon$ -irreducible if  $f$  cannot be expressed as  $f(x, y) = g(x, y)h(x, y) + \mathcal{E}(x, y)$  where  $h, g, \mathcal{E} \in \mathbb{F}[x, y]$  and  $\|\mathcal{E}(x, y)\| < \epsilon \|f(x, y)\|$ . Nevertheless we observe that taking, if necessary, a smaller  $\epsilon$  we can avoid the properness requirement on the degree and we can change the  $\epsilon$ -irreducibility of  $\mathcal{D}$  by irreducibility over  $\mathbb{C}$ . Thus, we will ask the planar curve  $\mathcal{D}$  to satisfy the following general conditions:

1.  $\mathcal{D}$  is an affine real plane algebraic curve over  $\mathbb{C}$
2.  $\mathcal{D}$  is irreducible over  $\mathbb{C}$ .
3.  $\mathcal{D}^\infty$  consists in  $d$  different points at infinity, where  $d = \deg(\mathcal{D})$ , note that this, in particular, implies that all points at infinity are regular, and the line at infinity is not tangent to  $\mathcal{D}$ .
4.  $(1 : 0 : 0), (0 : 1 : 0) \notin \mathcal{D}^h$  (where  $\mathcal{D}^h$  denotes the homogenization of  $\mathcal{D}$ ).

Let us mention that the condition  $(1 : 0 : 0), (0 : 1 : 0) \notin \mathcal{D}^h$  can always be achieved by performing a suitable affine orthogonal linear change of coordinates.

In this situation, we have the following algorithm.

**Algorithm:** Given a tolerance  $0 < \epsilon < 1$ , and  $\mathcal{D}$  satisfying the conditions imposed above, the algorithm decides whether  $\mathcal{D}$  is  $\epsilon$ -rational and, in the affirmative case, it computes a rational parametrization  $\overline{\mathcal{P}}(t)$  of a curve  $\overline{\mathcal{D}}$  whose real part is at finite Hausdorff distance of the real part of  $\mathcal{D}$  and such that  $\deg(\mathcal{D}) = \deg(\overline{\mathcal{D}})$ . Let  $f$  be defining polynomial of  $\mathcal{D}$  and  $F$  its homogenization.

- (1) Let  $d = \deg(\mathcal{D})$ . If  $d = 1$  output a polynomial parametrization of the line  $\mathcal{D}$ . If  $d = 2$  apply algorithm from [7] to  $\mathcal{D}$ .
- (2) Compute  $\mathfrak{C}^{\text{ord}} = \{\mathcal{C}luster_{r_i}(Q_i)\}_{i=1, \dots, s_1}$  and  $\mathfrak{C}^{\text{non}} = \{\mathcal{C}luster_{T_i}(M_i)\}_{i=1, \dots, s_2}$  of  $\mathcal{D}$ ; say  $Q_i = (q_{i,1} : q_{i,2} : 1)$ ,  $M_i := (m_{i,1} : m_{i,2} : 1)$  and  $T_i := (k_{i,1}, \dots, k_{i,\ell_i})$ .
- (3) If  $\epsilon\text{-genus}(\mathcal{D}) \neq 0$  RETURN “ $\mathcal{D}$  is not  $\epsilon$ -rational”. If  $s = 1$  one may apply the algorithm from [7] for the monomial case.

- (4) Determine the linear subsystem  $\mathcal{A}_{d-2}$  of adjoints to  $\mathcal{D}$ , of degree  $d-2$ , that has the non-ordinary singularities  $M_i$ , for  $i \in \{1, \dots, s_2\}$ , as base points. Let  $\mathcal{H}_{d-2}$  be the intersection of  $\mathcal{A}_{d-2}$  with the linear system of degree  $(d-2)$  given by the divisor  $\sum_{i=1}^s (r_i - 1)Q_i$ .
- (5) Compute  $(d-3)$   $\epsilon$ -ramification points  $\{P_j\}_{1 \leq j \leq d-3}$  of  $\mathcal{D}$ ; if there are not enough  $\epsilon$ -ramification points, complete with simple  $\epsilon$ -points. Take the points over  $\mathbb{R}$ , or as conjugate complex points. After each point computation check that it is not in the cluster of the others (including the clusters in  $\mathfrak{C}^{\text{ord}} \cup \mathfrak{C}^{\text{non}}$ ); if this fails take a new one. Say  $P_i = (p_{i,1} : p_{i,2} : 1)$ .
- (6) Determine the linear subsystem  $\mathcal{H}_{d-2}^*$  of  $\mathcal{H}_{d-2}$  given by the divisor  $\sum_{i=1}^{d-3} P_i$ . Let  $H^*(t, x, y, z) = H_1(x, y, z) + tH_2(x, y, z)$  be its defining polynomial.
- (7) If  $[\gcd(F(x, y, 0), H_1(x, y, 0)) \neq 1]$  and  $[\gcd(F(x, y, 0), H_2(x, y, 0)) \neq 1]$  replace  $H_2$  by  $H_2 + \rho_1 x^{d-2} + \rho_2 y^{d-2}$ , where  $\rho_1, \rho_2$  are real and strictly smaller than  $\epsilon$ . Say that  $\gcd(F(x, y, 0), H_2(x, y, 0)) = 1$ ; similarly in the other case.
- (8)  $S_1(x, t) = \text{Res}_y(H^*(x, y, 1), f)$  and  $S_2(y, t) = \text{Res}_x(H^*(x, y, 1), f)$ .
- (9)  $A_1 = \prod_{i=1}^{s_1} (x - q_{i,1})^{r_i(r_i-1)} \prod_{i=1}^{s_2} (x - m_{i,1})^{\sum_{j=1}^{\ell_i} k_{i,j}(k_{i,j}-1)} \prod_{i=1}^{d-3} (x - p_{i,1})$ ,  
 $A_2 = \prod_{i=1}^{s_1} (y - q_{i,2})^{r_i(r_i-1)} \prod_{i=1}^{s_2} (y - m_{i,2})^{\sum_{j=1}^{\ell_i} k_{i,j}(k_{i,j}-1)} \prod_{i=1}^{d-3} (y - p_{i,2})$ .
- (10) For  $i = 1, 2$  compute the quotient  $B_i$  of  $S_i$  by  $A_i$  w.r.t. either  $x$  or  $y$ .
- (11) If the content of  $B_1$  w.r.t  $x$  or the content of  $B_2$  w.r.t.  $y$  does depend on  $t$ , RETURN "degenerate case" (see [6]).
- (12) Determine the root  $\bar{p}_1(t)$  of  $B_1$ , as a polynomial in  $x$ , and the root  $\bar{p}_2(t)$  of  $B_2$ , as a polynomial in  $y$ .
- (12) RETURN  $\bar{\mathcal{P}}(t) = (\bar{p}_1(t), \bar{p}_2(t))$ .

In the following Example we illustrate the Algorithm.

**Example 3.1.** Let  $\epsilon = \frac{1}{100}$  and  $\mathcal{D}$  the curve of proper degree 5 defined by (see Fig.3.1):

$$f(x, y) = \frac{8578750}{617673396283947}y^3x^2 - \frac{299200}{7625597484987}yx^3 - \frac{1870000}{617673396283947}y^2x^2 + \frac{56359375}{50031545098999707}y^4x$$

$$- \frac{11687500}{150094635296999121}y^3x + \frac{17276000}{617673396283947}x^3y^2 - \frac{6055664500}{50031545098999707}x^4y - \frac{47872}{282429536481}x^4$$

$$+ \frac{1562500}{50031545098999707}y^5 + \frac{3125000}{50031545098999707}x^5.$$

First we compute the  $\epsilon$ -singularities of  $\mathcal{D}$ :

$$\{Q_1 = (0.008215206627 - 0.003422196305I, -0.1256431531 + 0.01292576399I),$$

$$Q_2 = (0.008215206627 + 0.003422196305I, -0.1256431531 - 0.01292576399I),$$

$$Q_3 = (0, 0), Q_4 = (0.003676621613, -0.05844533731), Q_5 = (0.02528071675, -0.2879266871)\}.$$

The singularities  $\{Q_1, Q_2\}$  have  $\epsilon$ -multiplicity 3, and  $\{Q_3, Q_4, Q_5\}$  have  $\epsilon$ -multiplicity 4. Moreover, the cluster decomposition of the singular locus consists in an unique cluster taking the maximum  $\epsilon$ -multiplicity 4:  $\mathcal{C}luster_4(Q_3) = \{Q_1, Q_2, Q_3, Q_4, Q_5\}$ . And therefore  $\mathcal{D}$  is  $\epsilon$ -rational since it is monomial. Finally, the algorithm outputs the parametrization:

$$\bar{\mathcal{P}}(t) = \left( \frac{748(25t + 324)^3}{375(t-2)(12500t^4 + 475875t^3 + 6510780t^2 + 24216408t - 12500)}, \right.$$

$$\left. t \frac{748(25t + 324)^3}{375(t-2)(12500t^4 + 475875t^3 + 6510780 * t^2 + 24216408t - 12500)} \right).$$

See the following figure to compare the input and the output curves:

**Acknowledgments:** This work was developed, and partially supported, under the research project MTM2011-25816-C02-01. All authors belong to the Research Group ASYNACS (Ref. CCEE2011/R34).

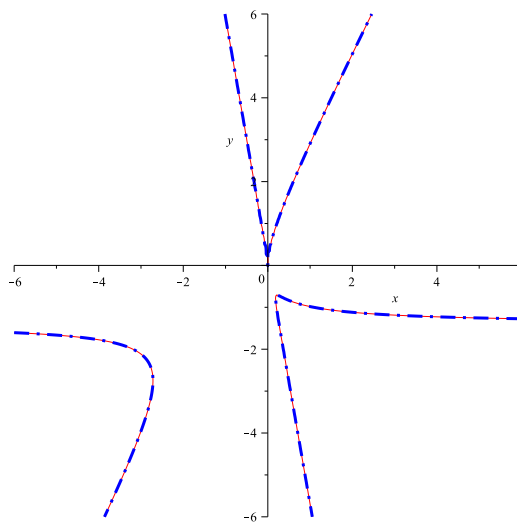


Figure 1: Input (in dots) and output curve.

## References

- [1] Aliprantis C.D., Border K.C. (2006). *Infinite Dimensional Analysis*. Springer Verlag.
- [2] Bai Y-B, Yong J-H, Liu C-Y, Liu X-M, Meng Y. (2011). *Polyline approach for approximating Hausdorff distance between planar free-form curves*. Computer-Aided Design. Vol. 43 Issue 6, pp. 687 - 698.
- [3] Bela Sz., Jüttler B. (2012). *Approximating Algebraic Space Curves by Circular Arcs*. Curves and Surfaces, 7th International Conference, Avignon 2010, Springer, J.-D. Boissonat et al., Lecture Notes in Computer Science 6920, pp. 157 - 177.
- [4] Bizzarri M., Lávička M., A symbolic-numerical approach to approximate parameterizations of space curves using graphs of critical points. Journal of Computational and Applied Mathematics (to appear).
- [5] Cheng J.S., Jim K., Gao X-S., Lazard D. (2012). *Certified Rational Parametric Approximation of Real Algebraic Space Curves with Local Generic Position Method*. arXiv: 1204.0905v1.
- [6] Pérez-Díaz S., Rueda S.L., Sendra J., Sendra J.R., (2010). *Approximate Parametrization of Plane Algebraic Curves by Linear Systems of Curves*. Computer Aided Geometric Design Vol. 27, pp. 212-231.
- [7] Pérez-Díaz S., Sendra J., Sendra J.R., (2004). *Parametrization of Approximate Algebraic Curves by Lines*. Theoretical Computer Science. Vol. 315/2-3. pp. 627 - 650.
- [8] Pérez-Díaz S., Sendra J., Sendra J.R., (2005). *Parametrization of Approximate Algebraic Surfaces by Lines*. Computer Aided Geometric Design. Vol. 22/2. pp. 147 - 181.
- [9] Rueda S.L., Sendra J., Sendra J.R., (2013). *An Algorithm to Parametrize Approximately Space Curves*. Journal of Symbolic Computation (to appear).
- [10] Rueda S.L., Sendra J., Sendra J.R., (2013). *Bounding and Estimating the Hausdorff distance between real space algebraic curves*, preprint.
- [11] Rueda S.L., Sendra J., Sendra J.R., (2013). *Rational Hausdorff Divisors: a New approach to the Approximate Parametrization of Curves*, preprint.

# Radical parametrization of algebraic curves and surfaces

J. Rafael Sendra

Dept. of Physics and Mathematics, University of Alcalá de Henares (Spain)

David Sevilla

Dept. of Mathematics, University of Extremadura (Spain)

sevillad@unex.es

## Abstract

Parametrization of algebraic curves and surfaces is a fundamental topic in CAGD (intersections; offsets and conchoids; etc.) There are many results on rational parametrization, in particular in the curve case, but the class of such objects is relatively small. If we allow root extraction, the class of parametrizable objects is greatly enlarged (for example, elliptic curves can be parametrized with one square root). We will describe the basics and the state of the art of the problem of parametrization of curves and surfaces by radicals.

## Keywords

Radical parametrization, parametrization of curves, parametrization of surfaces

## 1 Introduction

It is well known that the only algebraic curves that are rationally parametrizable are those of genus zero, and there are algorithms for that purpose (Sendra et al., 2008). However, in many applications, this is a strong limitation because either the curves appearing in the process are not rational (i.e. genus zero curves) or the algebraic manipulation of the geometric object does not preserve the genus; this happens, for instance, when applying offsetting constructions (Arrondo et al., 1997) or performing conchoidal transformations (Sendra and Sendra, 2010).

On the other hand, allowing radicals rather than just rational functions greatly enlarges the class of parametrizable functions. For example, one class of curves which are clearly parametrizable by radicals is that of hyperelliptic curves. Every such curve can be written as  $y^2 = P(x)$  for some polynomial  $P(x)$ , and we can quickly write the parametrization  $x = t, y = \sqrt{P(t)}$  where the root is meant to be taking in a strictly algebraic sense, that is, as an element of an algebraic extension of the field  $\mathbb{F}(t)$  where  $\mathbb{F}$  is the coefficient field of the curve. Essentially, a radical parametrization is given by rational functions whose numerators and denominators are radicals expressions of polynomials.

The roots of univariate polynomials of degree  $\leq 4$  can be written in terms of radicals. Therefore, curves which can be expressed as  $f(x, y) = 0$  where one of the variables occurs with degree  $\leq 4$  can also be parametrized by radicals. In relation to this, the minimum degree of a map from the curve to  $\mathbb{P}^1$  is called the *gonality* of the curve. Hyperelliptic curves are precisely those of gonality two and, as in the example above, can be parametrized using one square root. It is thus interesting to characterize the curves of gonality three (*trigonal*) and four (*trigonal*), and further to produce algorithms that detect these situations and compute a radical parametrization.

In relation to this, the following facts are relevant. In Zariski (1926), Zariski proved that the general complex projective curve of genus  $g > 6$  is not parametrizable by radicals. Moreover, as remarked in Pirola and Schlesinger (2005), Zariski's result is sharp. Indeed, a result within Brill-Noether theory (see Brill and Noether (1873), or (Arbarello et al., 1985, Chapter V) for a more modern account) states that a curve of genus  $g$  has a linear system of dimension 1 and degree  $\lceil \frac{g}{2} + 1 \rceil$  (Arbarello et al., 1985, p. 206), thus a map of that degree to  $\mathbb{P}^1$ . The previous expression is thus an upper bound for the gonality in terms of the genus. It follows that for  $g = 3, 4$  there exists generically a  $3 : 1$  map whose inversion would provide a radical parametrization with cubic



roots, and for  $g = 5, 6$  the inversion of the existing  $4 : 1$  would provide a radical parametrization with quartic roots. These are instances of trigonal and tetragonal curves.

We do not wish to enter the thorny realm of evaluation of radical functions, so we consider them as elements in an certain algebraic field extension, not as functions. For simplicity, let us restrict the discussion to the situations where the coefficient field is algebraically closed of characteristic zero.

## 2 The trigonal case

An algorithm for the trigonal case is described in Schicho and Sevilla (2012). The solution is based on the *Lie algebra method* introduced in de Graaf et al. (2006) (see also de Graaf et al. (2009)). There Lie algebra computations (which mostly amount to linear algebra) are used to decide if a certain algebraic variety associated to the input curve is a rational normal scroll, which is the case precisely when the curve is trigonal. Further, one can compute an isomorphism between that variety and the scroll when it exists.

Let  $C$  be an non-hyperelliptic algebraic curve of genus  $g \geq 4$ , so that it is isomorphic to its image by the canonical map  $\varphi: C \rightarrow \mathbb{P}^{g-1}$ . In Enriques (1919) and Babbage (1939) it is proven that  $\varphi(C)$  is the intersection of the quadrics that contain it, except when  $C$  is trigonal (that is, it has a  $g_3^1$ ) or isomorphic to a plane quintic ( $g = 6$ ). In those cases, the corresponding varieties are minimal degree surfaces, see (Griffiths and Harris, 1978, p. 522 and onwards).

From this situation we exclude the curves with genus lower than 3 since they are hyperelliptic, thus they have a  $g_2^1$  which can be made into a  $g_3^1$  by adding a base point; the problem is then to find a point in the curve over the field of definition. Also, if the curve is non-hyperelliptic of genus 3, it is isomorphic to its canonical image which is a quartic in  $\mathbb{P}^2$ , and the system of lines through any point of the curve cuts out a  $g_3^1$ .

The following theorem summarizes the classification of canonical curves according to the intersection of the quadric hypersurfaces that contain them.

**Theorem 1 (Griffiths and Harris (1978, p. 535))** *For any canonical curve  $C \subset \mathbb{P}^{g-1}$  over an algebraically closed field, either*

1.  $C$  is entirely cut out by quadric hypersurfaces; or
2.  $C$  is trigonal, in which case the intersection of all quadrics containing  $C$  is isomorphic to the rational normal scroll swept out by the trichords of  $C$ ; or
3.  $C$  is isomorphic to a plane quintic, in which case the intersection of the quadrics containing  $C$  is isomorphic to the Veronese surface in  $\mathbb{P}^5$ , swept out by the conic curves through five coplanar points of  $C$ .

There exist efficient algorithms for the computation of the canonical map, determination of hyperellipticity, and calculation of the space of forms of a given degree containing a curve, for example in Magma (Bosma et al., 1997) and at least partially in Maple. Thus the problem lies in *recognizing* which of the previous types is that of the intersection of the quadrics containing  $C$ .

**Definition 2** *Every finite-dimensional Lie algebra  $L$  can be written as a semidirect sum of two parts called a solvable part and a semisimple part. The latter is called a Levi subalgebra of  $L$ , and it is unique up to conjugation, so we will speak of “the” Levi subalgebra of  $L$  and denote it as  $LSA(L)$ . For a variety  $X$ , we will denote  $LSA(L(X))$  simply by  $LSA(X)$ .*

The Lie algebra of a curve of genus 2 or higher is zero since its automorphism group is finite. The rest of the cases that arise in Theorem 1 are studied in the next result.

**Theorem 3 (Oda (1988, Section 3.4))** *Let  $k$  be an algebraically closed field of characteristic zero. As above, let  $S_{m,n}$  be the the rational normal scroll with parameters  $m, n$ , and let  $V$  be the image of the Veronese map  $\mathbb{P}^2 \rightarrow \mathbb{P}^5$ .*

1.  $LSA(S_{m,n}) \cong \mathfrak{sl}_2$  if  $m \neq n$ .
2.  $LSA(S_{m,m}) \cong \mathfrak{sl}_2 + \mathfrak{sl}_2$  (a direct sum of two Lie algebras)
3.  $LSA(V) \cong \mathfrak{sl}_3$ .

Therefore, just by looking at the dimension of the Levi subalgebra we can discard the two cases where the curve is not trigonal. In other words, we can recognize a trigonal curve by the dimension of its Levi subalgebra.

**Corollary 4** *Let  $k$  be any field of characteristic zero, let  $C$  be a canonical curve and  $X$  be the intersection of the quadrics that contain it. Then one of the following occurs:*

- *If  $\dim LSA(X) = 0$  then  $X = C$  and  $C$  is not trigonal.*
- *If  $\dim LSA(X) = 3$  then  $X$  is a twist of  $S_{m,n}$  with  $m \neq n$  and  $C$  is trigonal.*
- *If  $\dim LSA(X) = 6$  then  $X$  is a twist of  $S_{m,m}$  and  $C$  is trigonal.*
- *If  $\dim LSA(X) = 8$  then  $X \cong V$  and  $C$  is not trigonal.*

### 3 The tetragonal case and higher gonality

For the cases of genus 5 and 6, a solution was presented in Harrison (2013) which involves the study of minimal free resolutions of certain geometric constructions. Unfortunately there has been no extension to tetragonal curves of arbitrary genus.

Very recently, in Schicho et al. (2013) the authors have published a deterministic algorithm that calculates the gonality of a given curve and a map to  $\mathbb{P}^1$  that realizes the gonality. The methods they use are based on syzygies, and are quite limited in practical computations. On the other hand, in (Schicho et al., 2013, Theorem 1.3) an algorithm for the case of gonality up to 4 for curves in characteristic  $\neq 2, 3$ .

Although these results allow us to find lowest degree maps, their invertibility by radicals is generally not possible outside the cases discussed above.

### 4 Parametrization by lines and adjoints

A more direct approach for particular cases is shown in Sendra and Sevilla (2011). First, it is established that the construction of offsets and conchoids, two common constructions in CAGD, is closed under parametrizability by radicals. That is, an offset or conchoid constructed over a curve that is parametrizable by radicals will also be a curve of such type. Another class of curves that can be quickly parametrized by radicals are those of degree  $d$  and possessing a point of multiplicity  $d - r$  for some  $r \leq 4$ ; in this situation one can produce the parametrization by considering a pencil of lines through the point. Finally, by employing adjoint curves as it is done in the rational case, it is possible to parametrize by radicals curves of genus up to 4.

The caveat is that this method produces  $g : 1$  maps where  $g$  is the genus. This means that trigonal curves of genus 4 are parametrized by quartic roots, although they can be parametrized by cubic roots; analogously, for curves of genus 5 or 6 a quintic or sextic polynomial in one variable needs to be resolved by radicals in order to produce a parametrization, whereas we know that they can be parametrized by quartic roots.

In any case, these methods provide efficient radical parametrizations for curves that are of practical interest.

### 5 Radical parametrization of surfaces

It is possible to exploit the results outlined in the previous section for the case of surfaces. As in the curve case, only a narrow class of algebraic surfaces can be parametrized rationally. Namely, the two genera must be zero. What follows is taken from Sendra and Sevilla (2013).

However, by using resolution of univariate polynomials by radicals, it is clear that one can parametrize several new classes of surfaces by radicals. For example, if a surface is given as the zeros of  $F(x,y,z)$  where the degree of any of the variables is less or equal than 4, we can parametrize by solving  $F$  as a univariate polynomial.

In a more geometric fashion, a surface of degree  $d$  that possess a point of multiplicity  $d - r$  for some  $r \leq 4$  can be parametrized by the pencil of lines through the point. Therefore, every surface of degree 5 is parametrizable by radicals, and so is every singular surface of degree 6.

If we regard  $F(x, y, z)$  as a polynomial in  $x, y$  with coefficients in  $\mathbb{F}(z)$ , we can use the parametrization by adjoints methods of the previous section. The caveat here is that, if the relevant construction employs a point in the curve case (not problematic since our coefficient field is algebraically closed), in the surface case it is necessary that there exist such a point satisfying that its coordinates are radical functions. Otherwise, the parametrization we obtain would be radical in  $x, y$  but not in  $z$ . This produces several cases depending on the genus of  $F(x, y)(z)$  and the existence of points with the property just mentioned.

Finally, as in the curve case, certain geometric constructions are proven to be closed under parametrizability by radicals.

## Acknowledgements

This contribution is partially supported by the Ministerio de Economía y Competitividad under the project MTM2011-25816-C02-01, by the Austrian Science Fund (FWF) P22766-N18, and by Junta de Extremadura and FEDER funds. The first author is a member of the of the Research Group ASYNACS (Ref. CCEE2011/R34).

## References

- Arbarello, E., Cornalba, M., Griffiths, P.A., Harris, J., 1985. Geometry of algebraic curves. Vol. I. volume 267 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, New York.
- Arrondo, E., Sendra, J., Sendra, J.R., 1997. Parametric generalized offsets to hypersurfaces. *J. Symbolic Comput.* 23, 267–285. Parametric algebraic curves and applications (Albuquerque, NM, 1995).
- Babbage, D.W., 1939. A note on the quadrics through a canonical curve. *J. London Math. Soc.* 14, 310–315.
- Brill, A., Noether, M., 1873. ber die algebraischen functionen und ihre anwendungen in der geometrie. *Math. Ann.* 7, 269–310.
- Bosma, W., Cannon, J., Playoust, C., 1997. The Magma algebra system. I. The user language. *J. Symbolic Comput.* 24, 235–265. Computational algebra and number theory (London, 1993).
- de Graaf, W.A., Harrison, M., Pílníková, J., Schicho, J., 2006. A Lie algebra method for rational parametrization of Severi-Brauer surfaces. *J. Algebra* 303, 514–529.
- de Graaf, W.A., Pílníková, J., Schicho, J., 2009. Parametrizing del Pezzo surfaces of degree 8 using Lie algebras. *J. Symbolic Comput.* 44, 1–14.
- Enriques, F., 1919. Sulle curve canoniche di genere  $p$  dello spazio a  $p - 1$  dimensioni. *Rend. Accad. Sci. Ist. Bologna* , 80–82.
- Griffiths, P., Harris, J., 1978. Principles of algebraic geometry. Wiley-Interscience [John Wiley & Sons], New York. Pure and Applied Mathematics.
- Harrison, M., 2013. Explicit solution by radicals, gonal maps and plane models of algebraic curves of genus 5 or 6. *J. Symbolic Comput.* 51, 3–21.
- Oda, T., 1988. Convex bodies and algebraic geometry. volume 15 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin. An introduction to the theory of toric varieties, Translated from the Japanese.
- Pirola, G.P., Schlesinger, E., 2005. A curve algebraically but not rationally uniformized by radicals. *J. Algebra* 289, 412–420.
- Schicho, J., Schreyer, F.O., Weimann, M., 2013. Computational aspects of gonal maps and radical parametrization of curves. ArXiv: math.AG/1304.2551v1.

- Schicho, J., Sevilla, D., 2012. Effective radical parametrization of trigonal curves, in: Computational algebraic and analytic geometry. Amer. Math. Soc., Providence, RI. volume 572 of *Contemp. Math.*, pp. 221–231.
- Sendra, J.R., Sendra, J., 2010. Rational parametrization of conchoids to algebraic curves. *Appl. Algebra Engrg. Comm. Comput.* 21, 285–308.
- Sendra, J.R., Sevilla, D., 2011. Radical parametrizations of algebraic curves by adjoint curves. *J. Symbolic Comput.* 46, 1030–1038.
- Sendra, J.R., Sevilla, D., 2013. First steps towards radical parametrization of algebraic surfaces. *Comput. Aided Geom. Design* 30, 374–388.
- Sendra, J.R., Winkler, F., Pérez-Díaz, S., 2008. Rational algebraic curves. volume 22 of *Algorithms and Computation in Mathematics*. Springer, Berlin. A computer algebra approach.
- Zariski, O., 1926. Sull'impossibilità di risolvere parametricamente per radicali un'equazione algebrica  $f(x, y) = 0$  di genere  $p > 6$  a moduli generali. *Atti Accad. Naz. Lincei Rend., Cl. Sc. fis. Mat. Natur., serie VI* 3, 660–666.

# Classification of $q$ -Weierstrass points for hyperelliptic curves of genus 3

Tony Shaska  
Oakland University, Rochester, MI, USA.

Caleb Shor  
Western New England University, Springfield, MA, USA.

shaska@oakland.edu

## Abstract

Let  $C$  be a genus 3 hyperelliptic curve with an elliptic involution. Then  $C$  has equation  $y^2 = x^8 + ax^6 + bx^4 + cx^2 + 1$  for constants  $a, b, c$ . Associated to these curves are dihedral invariants  $\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4$  which uniquely determine the isomorphism classes of these curves. In this paper, we aim to classify the  $q$ -Weierstrass points of these curves in terms of such invariants.

## Keywords

Weierstrass points,  $q$ -Weierstrass points, genus 3 hyperelliptic curves, invariants

## 1 Introduction

The Riemann-Roch theorem shows that every point on a genus  $g \geq 2$  curve has a non-constant function associated to it which has a pole of order less than or equal to  $g + 1$  and no other poles. A *Weierstrass point* is a point such that there is a non-constant function which has a low order pole and no other poles. By “low order” we mean a pole of order at most  $g$ . A  $q$ -*Weierstrass point*, for any  $q \in \mathbb{N}$ , is a point which has a higher than expected order of vanishing in a space of holomorphic  $q$ -differentials.

Hurwitz showed that all Weierstrass points on a given curve are zeroes of a certain high order differential form. The *Weierstrass weight* of a point is the order of the zero of this form at the point. Since this differential form has degree  $g^3 - g$  then there are only finitely many Weierstrass points.

In a similar manner, the  $q$ -Weierstrass points are zeroes of a certain high order differential form. The Weierstrass  $q$ -weight is the order of the zero, and as above, there are finitely many  $q$ -Weierstrass points.

Let  $C$  be a genus 3 hyperelliptic curve with an elliptic involution. Then,  $C$  has equation

$$y^2 = x^8 + ax^6 + bx^4 + cx^2 + 1.$$

The dihedral invariants  $\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4$  as defined in [5] uniquely determine the isomorphism class of such curves.

The goal of this paper is to classify all Weierstrass and  $q$ -Weierstrass points and their weights in terms of such invariants.

## 2 Genus 3 hyperelliptic fields with elliptic involutions

Let  $K$  be a genus 3 hyperelliptic field. Then  $K$  has exactly one genus 0 subfield of degree 2, call it  $k(X)$ . It is the fixed field of the **hyperelliptic involution**  $\omega_0$  in  $\text{Aut}(K)$ . Thus,  $\omega_0$  is central in  $\text{Aut}(K)$ , where  $\text{Aut}(K)$  denotes the group  $\text{Aut}(K/k)$ . It induces a subgroup of  $\text{Aut}(k(X))$  which is naturally isomorphic to  $\overline{\text{Aut}}(K) := \text{Aut}(K)/\langle \omega_0 \rangle$ . The latter is called the **reduced automorphism group** of  $K$ .

**Definition 1.** An *elliptic involution* (or *non-hyperelliptic*) of  $G = \text{Aut}(K)$  is an involution different from  $\omega_0$ . Thus, the elliptic involutions of  $G$  are in 1-1 correspondence with the non-hyperelliptic subfields of  $K$  of degree 2.

Let  $\varepsilon$  be a non-hyperelliptic involution in  $\bar{G}$ . We can choose the generator  $X$  of  $\text{Fix}(\omega_0)$  such that  $\varepsilon(X) = -X$ . Then  $K = k(X, Y)$  where  $X, Y$  satisfy equation

$$Y^2 = (X^2 - \alpha_1^2)(X^2 - \alpha_2^2)(X^2 - \alpha_3^2)(X^2 - \alpha_4^2) \quad (1)$$

for some  $\alpha_i \in k$ ,  $i = 1, \dots, 4$ . Denote by

$$\begin{aligned} s_1 &= -(\alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_4^2) \\ s_2 &= (\alpha_1\alpha_2)^2 + (\alpha_1\alpha_3)^2 + (\alpha_1\alpha_4)^2 + (\alpha_2\alpha_3)^2 + (\alpha_2\alpha_4)^2 + (\alpha_3\alpha_4)^2 \\ s_3 &= -(\alpha_1\alpha_2\alpha_3)^2 - (\alpha_4\alpha_1\alpha_2)^2 - (\alpha_4\alpha_3\alpha_1)^2 - (\alpha_4\alpha_3\alpha_2)^2 \\ s_4 &= -(\alpha_1\alpha_2\alpha_3\alpha_4)^2 \end{aligned} \quad (2)$$

Then, we have

$$Y^2 = X^8 + s_1X^6 + s_2X^4 + s_3X^2 + s_4$$

with  $s_1, s_2, s_3, s_4 \in k$ ,  $s_4 \neq 0$ . Further  $E_1 = k(X^2, Y)$  and  $C = k(X^2, YX)$  are the two subfields corresponding to  $\varepsilon$  of genus 1 and 2 respectively.

Preserving the condition  $\varepsilon(X) = -X$  we can further modify  $X$  such that  $s_4 = 1$ . Then, we have the following:

The following Lemma is proven in [5].

**Lemma 1.** Every genus 3 hyperelliptic curve  $\mathcal{X}$ , defined over a field  $k$ , which has a non-hyperelliptic involution has equation

$$Y^2 = X^8 + aX^6 + bX^4 + cX^2 + 1 \quad (3)$$

for some  $a, b, c \in k^3$ , where the polynomial on the right has non-zero discriminant.

The above conditions determine  $X$  up to coordinate change by the group  $\langle \tau_1, \tau_2 \rangle$  where

$$\tau_1 : X \rightarrow \zeta_8 X, \quad \text{and} \quad \tau_2 : X \rightarrow \frac{1}{X},$$

and  $\zeta_8$  is a primitive 8-th root of unity in  $k$ . Hence,

$$\tau_1 : (a, b, c) \rightarrow (\zeta_8^6 a, \zeta_8^4 b, \zeta^2 c),$$

and

$$\tau_2 : (a, b, c) \rightarrow (c, b, a).$$

Then,  $|\tau_1| = 4$  and  $|\tau_2| = 2$ . The group generated by  $\tau_1$  and  $\tau_2$  is the dihedral group of order 8. Invariants of this action are

$$\begin{aligned} \mathfrak{s}_2 &= ac, \\ \mathfrak{s}_3 &= (a^2 + c^2)b, \\ \mathfrak{s}_4 &= a^4 + c^4, \end{aligned} \quad (4)$$

since

$$\begin{aligned} \tau_1(a^4 + c^4) &= (\zeta_8^6 a)^4 + (\zeta_8^2 c)^4 = a^4 + c^4 \\ \tau_1((a^2 + c^2)b) &= (\zeta_8^4 a^2 + \zeta_8^4 c^2) \cdot (\zeta_8^4 b) = (a^2 + c^2)b \\ \tau_1(ac) &= \zeta_8^6 a \cdot \zeta_8^2 c = ac \end{aligned}$$

Since they are symmetric in  $a$  and  $c$ , then they are obviously invariant under  $\tau_2$ . Notice that  $\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4$  are homogenous polynomials of degree 2, 3, and 4 respectively. The subscript  $i$  represents the degree of the polynomial  $\mathfrak{s}_i$ .

Since the above transformations are automorphisms of the projective line  $\mathbb{P}^1(k)$  then the  $SL_2(k)$  invariants must be expressed in terms of  $\mathfrak{s}_4, \mathfrak{s}_3$ , and  $\mathfrak{s}_2$ . In these parameters, the discriminant of the octavic polynomial on the right hand side of Eq. (3) equals  $-\frac{256}{(\mathfrak{s}_4+2\mathfrak{s}_2^2)^4} \Delta^2$ , where

$$\begin{aligned} \Delta = & 132\mathfrak{s}_2^4\mathfrak{s}_4 - 18\mathfrak{s}_4^2\mathfrak{s}_2\mathfrak{s}_3 - 72\mathfrak{s}_4\mathfrak{s}_2^3\mathfrak{s}_3 - \mathfrak{s}_4\mathfrak{s}_2^2\mathfrak{s}_3^2 + 80\mathfrak{s}_2\mathfrak{s}_3^2\mathfrak{s}_4 - 576\mathfrak{s}_3\mathfrak{s}_2^2\mathfrak{s}_4 \\ & - 256\mathfrak{s}_4^2 + 768\mathfrak{s}_4\mathfrak{s}_2^3 - 1024\mathfrak{s}_4\mathfrak{s}_2^2 + 256\mathfrak{s}_2^2\mathfrak{s}_3^2 - 576\mathfrak{s}_2^4\mathfrak{s}_3 + 768\mathfrak{s}_2^5 + 24\mathfrak{s}_2^6 \\ & - 16\mathfrak{s}_3^4 - 1024\mathfrak{s}_2^4 + 128\mathfrak{s}_3^2\mathfrak{s}_4 + 192\mathfrak{s}_4^2\mathfrak{s}_2 + 114\mathfrak{s}_4^2\mathfrak{s}_2^2 + 4\mathfrak{s}_4^2\mathfrak{s}_2^3 - 144\mathfrak{s}_4^2\mathfrak{s}_3 \\ & + 16\mathfrak{s}_4\mathfrak{s}_2^5 - 72\mathfrak{s}_2^5\mathfrak{s}_3 - 2\mathfrak{s}_2^4\mathfrak{s}_3^2 + 160\mathfrak{s}_2^3\mathfrak{s}_3^2 + 4\mathfrak{s}_3^3\mathfrak{s}_4 + 8\mathfrak{s}_3^3\mathfrak{s}_2^2 + 27\mathfrak{s}_4^3 + 16\mathfrak{s}_2^7 \end{aligned} \quad (5)$$

The map

$$(a, b, c) \mapsto (\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4)$$

is a branched Galois covering with group  $D_4$  of the set

$$\{(\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4) \in k^3 : \Delta_{(\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4)} \neq 0\}$$

by the corresponding open subset of  $a, b, c$ -space. In any case, it is true that if  $a, b, c$  and  $a', b', c'$  have the same  $\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4$ -invariants then they are conjugate under  $\langle \tau_1, \tau_2 \rangle$ .

The case when  $\mathfrak{s}_3 = 0$  must be treated separately. We have two sub cases  $a^2 + c^2 = 0$  or  $b = 0$ . Then we define new invariants as follows:

$$\mathfrak{p}(\mathcal{X}_3) = \begin{cases} w = b^2 & \text{if } a = c = 0, \\ (\mathfrak{s}_2, w, \mathfrak{s}_4) & \text{if } a^2 + c^2 = 0 \text{ and } b \neq 0, \\ (\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4) & \text{otherwise.} \end{cases} \quad (6)$$

We denote by  $\mathcal{M}_3^b$  the locus of bielliptic curves in  $\mathcal{M}_3$  and by  $\mathcal{H}_3$  the hyperelliptic locus. The following theorem is proved in [5].

**Theorem 1.** *Let  $\mathcal{X}$  be a curve in  $\mathcal{S} = \mathcal{M}_3^b \cap \mathcal{H}_3$ . Then, one of the following occurs:*

- i) *Aut  $(\mathcal{X}) \cong \mathbb{Z}_2^3$  if and only if  $\mathfrak{s}_4 - 2\mathfrak{s}_2^2 = 0$*
- ii) *Aut  $(\mathcal{X}) \cong \mathbb{Z}_2 \times D_8$  if and only if  $\mathfrak{s}_2 = \mathfrak{s}_4 = 0$*
- iii) *Aut  $(\mathcal{X}) \cong \mathbb{Z}_2 \times \mathbb{Z}_4$  if and only if  $\mathfrak{s}_4 + 2\mathfrak{s}_2^2 = 0$  and  $\mathfrak{s}_3 = 0$ .*
- iv) *Aut  $(\mathcal{X}) \cong D_{12}$  if and only if*

$$\begin{aligned} \mathfrak{s}_3 &= \frac{1}{75} (9\mathfrak{s}_2 - 224)(\mathfrak{s}_2 - 196) \\ \mathfrak{s}_4 &= -\frac{9}{125}\mathfrak{s}_2^3 + \frac{1962}{125}\mathfrak{s}_2^2 - \frac{840448}{1125}\mathfrak{s}_2 + \frac{9834496}{1125}. \end{aligned} \quad (7)$$

## 3 Weierstrass and $q$ -Weierstrass points of curves

### 3.1 Weierstrass points

Following the notation of [6], let  $k$  be an algebraically closed field, and let  $C$  be a non-singular projective curve over  $k$  of genus  $g$ . Let  $k(C)$  be the associated function field. For any divisor  $D$  on  $C$ , let  $\mathcal{L}(D) = \{f \in k(C) : (f) + D \geq 0\} \cup \{0\}$ . Let  $\ell(D) = \dim_k(\mathcal{L}(D))$ . By Riemann-Roch, for any canonical divisor  $K$ , we have

$$\ell(D) - \ell(K - D) = \deg(D) + 1 - g.$$

Since  $\deg(K) = 2g - 2$ , if  $\deg(D) \geq 2g - 1$ , we have

$$\ell(D) = \deg(D) + 1 - g.$$

Let  $P$  be a degree 1 point on  $C$ . Consider the chain of vector spaces

$$\mathcal{L}(0) \subseteq \mathcal{L}(P) \subseteq \mathcal{L}(2P) \subseteq \mathcal{L}(3P) \subseteq \dots \subseteq \mathcal{L}((2g-1)P).$$

Since  $\mathcal{L}(0) = k$ , we have  $\ell(0) = 1$ . And  $\ell((2g-1)P) = g$ . We obtain the corresponding sequence

$$\ell(0), \ell(P), \ell(2P), \ell(3P), \dots, \ell((2g-1)P).$$

It is straightforward to show that  $0 \leq \ell(nP) - \ell((n-1)P) \leq 1$  for all  $n \in \mathbb{N}$ . If  $\ell(nP) = \ell((n-1)P)$ , then we call  $n$  a gap number. For any point  $P$ , there are exactly  $g$  gap numbers. If the gap numbers are  $1, 2, \dots, g$ , then  $P$  is an *ordinary point*. Otherwise, we call  $P$  a *Weierstrass point*. (Equivalently, we call  $P$  a Weierstrass point if  $\ell(gP) > 1$ .)

### 3.2 $q$ -Weierstrass points

Using differentials, we can define  $q$ -Weierstrass points as in [2] and [1]. For any  $q \in \mathbb{N}$ , let  $H^0(C, (\Omega^1)^q)$  be the  $\mathbb{C}$ -vector space of holomorphic  $q$ -differentials on  $C$ . Let  $s = \dim(H^0(C, (\Omega^1)^q))$ .

As before, let  $P$  be a degree 1 point on  $C$ . Take a basis  $\{\psi_1, \dots, \psi_s\}$  of  $H^0(C, (\Omega^1)^q)$  such that  $\text{ord}_P(\psi_1) < \text{ord}_P(\psi_2) < \dots < \text{ord}_P(\psi_s)$ . For  $i = 1, \dots, s$ , let  $n_i = \text{ord}_P(\psi_i) + 1$ . The sequence of natural numbers  $G^{(q)}(P) = \{n_1, n_2, \dots, n_s\}$  is called the  $q$ -gap sequence of  $P$ . With such a gap sequence, we can calculate the  $q$ -weight of  $P$ , which is

$$w^{(q)}(P) = \sum_{i=1}^s (n_i - i).$$

We call the point  $P$  a  $q$ -Weierstrass point if  $w^{(q)}(P) > 0$ , and we let  $W_q(C)$  denote the set of all  $q$ -Weierstrass points on  $C$ . In particular,  $W_1(C)$ , the set of 1-Weierstrass points on  $C$ , is exactly the set of Weierstrass points as defined above in terms of Riemann-Roch.

Given a basis  $\{\psi_1, \dots, \psi_s\}$  of holomorphic differentials, where  $\psi_i = f_i(x)dx$  for a holomorphic function  $f_i$  of a local coordinate  $x$  for each  $i$ , the *Wronskian* is the determinant of the following  $s \times s$  matrix:

$$W = \begin{vmatrix} f_1(x) & f_2(x) & \cdots & f_s(x) \\ f_1'(x) & f_2'(x) & \cdots & f_s'(x) \\ \vdots & \vdots & \ddots & \vdots \\ f_1^{(s-1)}(x) & f_2^{(s-1)}(x) & \cdots & f_s^{(s-1)}(x) \end{vmatrix}.$$

The Wronskian form is  $\Omega_q = W(dx)^m$ , for

$$\begin{aligned} m &= q + (q+1) + (q+2) + \cdots + (q+s-1) \\ &= (s/2)(2q-1+s). \end{aligned}$$

Suppose  $P$  is a zero of order  $n$  for the form  $\Omega_q$ . Then  $P$  is a  $q$ -Weierstrass point with  $q$ -weight  $n$ . Since the Wronskian form is a holomorphic  $m$ -differential,  $\text{div}(\Omega_q)$  is effective. Thus, the  $q$ -Weierstrass points are the support of  $\text{div}(\Omega_q)$ , and the sum of the  $q$ -weights of the  $q$ -Weierstrass points is the degree of  $\text{div}(\Omega_q)$ , which is  $m(2g-2) = s(2q-1+s)(g-1)$ . In particular, this means there are a finite number of  $q$ -Weierstrass points.

## 4 Computations with genus $g = 3$

Let  $C$  be a hyperelliptic curve of genus  $g = 3$  with non-hyperelliptic, as in Eq. (3). As in Eq. (1), let  $\{\pm\alpha_1, \pm\alpha_2, \pm\alpha_3, \pm\alpha_4\}$  denote the 8 distinct roots of  $f(x)$ , and denote the corresponding ramification points on  $C$  by  $R_i^\pm = (\pm\alpha_i, 0)$ . Throughout this section, let  $w \in \mathbb{C}$  denote any non-root of  $f(x)$ , and let  $P_1^w$  and  $P_2^w$  denote the two (distinct) points above  $w$ . And let  $P_1^\infty$  and  $P_2^\infty$  denote the two points over  $\infty$  in the non-singular model of  $C$ .

Consider  $H^0(C, (\Omega^1)^q)$ , the space of holomorphic  $q$ -differentials on  $C$ . For a curve of genus  $g$ , by Riemann-Roch one has that  $\dim(H^0(C, (\Omega^1)^q)) = g$  and, for  $q \geq 2$ ,

$$\dim(H^0(C, (\Omega^1)^q)) = (g-1)(2q-1).$$

In particular, for  $g = 3$ , when  $q \geq 2$ ,  $\dim(H^0(C, (\Omega^1)^q)) = (4q-2)$ .

### 4.1 1-Weierstrass points

For  $q = 1$ , a basis of holomorphic 1-differentials is  $\left\{ \frac{1}{y}dx, \frac{(x-\beta)}{y}dx, \frac{(x-\beta)^2}{y}dx \right\}$  for any constant  $\beta \in \mathbb{C}$ . Using  $\beta = \pm\alpha_i$ , the 1-gap sequence of each branch point  $R_i^\pm$  is  $\{1, 3, 5\}$ , so the branch points have 1-weight 3. Using  $\beta = w$ , the finite non-branch points  $P_i^w$  have 1-gap sequence  $\{1, 2, 3\}$ , so 1-weight 0. And using any value of  $\beta$ , one finds the points at infinity  $P_i^\infty$  have 1-gap sequence  $\{1, 2, 3\}$ , so 1-weight 0. Hence, the 1-Weierstrass points are exactly the ordinary Weierstrass points.

The Wronskian form for  $q = 1$  is  $\Omega_1 = W(dx)^6$ , where  $W = 2/y^3$ . The associated divisor is

$$\begin{aligned} \text{div}(\Omega_1) &= \text{div}(2/y^3) + \text{div}(dx^6) \\ &= -3 \left( \sum_{i=1}^4 R_i^\pm - 4(P_1^\infty + P_2^\infty) \right) + 6 \left( \sum_{i=1}^4 R_i^\pm - 2(P_1^\infty + P_2^\infty) \right) = 3 \left( \sum_{i=1}^4 R_i^\pm \right), \end{aligned}$$

again showing that the branch points are the only 1-Weierstrass points, each with 1-weight equal to 3.



## 4.2 2-Weierstrass points

For any  $q \geq 2$ , a basis for  $H^0(C, (\Omega^1)^q)$  is

$$\left\{ \frac{(x-\beta)^i}{y^q} dx^q : 0 \leq i \leq 2q \right\} \cup \left\{ \frac{(x-\beta)^i (y-f_4(x))}{y^q} : 0 \leq i \leq 2q-4 \right\}$$

for any constant  $\beta$  and any polynomial  $f_4(x)$  with  $\deg(f) \leq 4$ . Letting  $\beta = \pm\alpha_i$  and  $f_4(x) = 1$ , one finds that the branch points have  $q$ -gap sequence  $\{1, 2, 3, \dots, 4q-6, 4q-5, 4q-3, 4q-1, 4q+1\}$ , so  $q$ -weight 6.

Now, let  $q = 2$  and let  $P = (w, z)$  be a non-branch point. Recall that  $\dim(H^0(C, (\Omega^1)^2)) = 6$ . For  $1 \leq i \leq 5$ , let  $\psi_i = \frac{(x-w)^{i-1}}{y^2} dx^2$ . For each  $i$ ,  $n_i = \text{ord}_P(\psi_i) + 1 = i$ , so the first five terms of the 2-gap sequence of  $P$  are  $\{1, 2, 3, 4, 5\}$ . As a sixth basis element, we take  $\frac{y-P_4(x)}{y^2} dx^2$ , where  $P_4(x)$  is the degree-4 Taylor polynomial to  $C$  at  $x = w$ . (Note that  $P_4(x)$  is well defined if  $P$  is not a branch point because  $\frac{dy}{dx}|_{x=w} \neq \infty$ .)

By construction,  $\text{ord}_P(y - P_4(x)) \geq 5$ . The sixth term of the 2-gap sequence is  $n_6 = \text{ord}_P(y - P_4(x)) + 1$ . Thus, if  $\text{ord}_P(y - P_4(x)) > 5$ , then  $P$  is a 2-Weierstrass point with 2-weight  $n_6 - 6 = \text{ord}_P(y - P_4(x)) - 5$ . Using the Taylor series for  $(y - P_4(x))$  at  $x = w$ , one can calculate the order of vanishing and hence the 2-weight. In particular,  $\text{ord}_P(y - P_4(x)) > 5$  if and only if  $\Phi_5(w) = 0$ , where  $\Phi_5(w)$  is a polynomial of degree at most 29 (depending on the values of  $\mathfrak{s}_2, \mathfrak{s}_3, \mathfrak{s}_4$ ).

To compute the 2-Weierstrass points with the Wronskian, we can use as a basis  $\psi_i$  as above for  $1 \leq i \leq 5$  and  $\psi_6 = (y/y^2)(dx)^2$ . A computation of the  $6 \times 6$  determinant with Mathematica gives  $\Omega_2 = c_0(\Phi(x)/y^{21})(dx)^{27}$  for a constant  $c_0$  and  $\Phi(x)$  the polynomial  $\Phi_5$  from above. Thus, the 2-Weierstrass points are the zeroes of  $\Omega_2$ , which has divisor

$$\text{div}(\Omega_2) = \text{div}(\Phi(x))_0 + 3 \left( \sum_{i=4}^4 R_i^\pm \right) + (30 - \deg(\Phi))(P_1^\infty + P_2^\infty).$$

We conclude that the eight branch points have 2-weight 3, the two points at infinity have 2-weight at least 1 (depending on the degree of  $\Phi(x)$ ), and the zeros of  $\Phi(x)$  have 2-weight according to the order of vanishing of  $\Phi(x)$ .

In [3] we aim to classify the 2-weights of 2-Weierstrass points on curves with automorphism groups as described in Theorem 1. An account for all superelliptic curves of higher genus is intended in [4].

## References

- [1] Mohamed Farahat and Fumio Sakai. The 3-Weierstrass points on genus two curves with extra involutions. *Saitama Math. J.*, 28:1–12 (2012), 2011.
- [2] H. M. Farkas and I. Kra. *Riemann surfaces*, volume 71 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1992.
- [3] T. Shaska and C. Shor. Weierstrass points of genus 3 hyperelliptic curves with elliptic involutions. *In progress*, 2013.
- [4] T. Shaska and C. Shor. Weierstrass points of some superelliptic curves via their dihedral invariants. *In progress*, 2013.
- [5] T. Shaska and F. Thompson. Bielliptic curves of genus 3 in the hyperelliptic moduli. *to appear*, 2013.
- [6] Henning Stichtenoth. *Algebraic function fields and codes*, volume 254 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, second edition, 2009.



---

---

# Session 7: Applications and Libraries development in DERIVE and TI-NSPIRE

---

---

**Organizers:**

José Luis Galán García  
Pedro Rodríguez Cielos  
Gabriel Aguilera Venegas  
Josef Böhm



# FOPDE.mth: Solving First-Order Partial Differential Equations with DERIVE 6 step by step

Gabriel Aguilera, José Luis Galán, María Ángeles Galán,  
Yolanda Padilla, Pedro Rodríguez  
University of Málaga (Spain)

Ricardo Rodríguez  
Technical University of Madrid

`jl_galan@uma.es`

## Abstract

A basic course in Partial Differential Equations (PDE) in Engineering, usually deals, at least, with the following 3 different first-order PDE problems:

1. **Pfaff Differential Equations**, which consists on finding the general solution for:

$$P(x, y, z) dx + Q(x, y, z) dy + R(x, y, z) dz = 0$$

2. **Quasi-linear Partial Differential Equations**, which consists on finding the general solution for:

$$P(x, y, z) p + Q(x, y, z) q = R(x, y, z)$$

where  $p = \frac{\partial z}{\partial x}$  and  $q = \frac{\partial z}{\partial y}$ .

3. Using **Lagrange-Charpit Method** for finding a *complete integral* for a given general first order partial differential equation:  $F(x, y, z, p, q) = 0$ .

In this lecture we will describe the file `FOPDE.mth`, developed in DERIVE 6 in order to solve these three problems (their general cases and the particular cases). Since these three problems requires several steps for their resolution, the programs developed in `FOPDE.mth` show step by step all the steps providing in this way a powerful tool as a tutorial for teaching how to solve these types of equations. This fact make possible the use of DERIVE 6 as a PECAS (Pedagogical CAS) providing not only the final result but also all partial results.

On the other hand, in order to deal with such equations, the resolution of first-order Ordinary Differential Equations (ODE) is needed. Therefore, `FOPDE.mth` loads the package `FOODE.mth`, which is part of the DERIVE package that was introduced in the “Computer Algebra in Education” Special Session at ACA 2008 ([1]).

Finally, we will state the conclusions obtained after using this file with our students and also some future work on this and other related subjects.

## Keywords

ODEs, PDEs, DERIVE, CAS, Pedagogical Computer Algebra System (PECAS), Engineering

## References

- [1] Gabriel Aguilera, José Luis Galán, M. Ángeles Galán, Antonio Gálvez, Antonio J. Jiménez, Yolanda Padilla, Pedro Rodríguez. DIFFERENTIAL EQUATIONS WITH DERIVE 6. Applications of Computer Algebra Conference, ACA 2008, [http://math.unm.edu/~aca/ACA/2008/Proceedings/Education/Galan\\_abstract.pdf](http://math.unm.edu/~aca/ACA/2008/Proceedings/Education/Galan_abstract.pdf).

# Integration of Piecewise Continuous Functions (Part I, Part II)

Michel Beaudin, Frédéric Henri, Geneviève Savard  
École de technologie supérieure (Canada)

`michel.beaudin@etsmtl.ca`

## Abstract

Piecewise functions are important in applied mathematics and engineering students need to deal with them often. In Nspire CAS, templates are an easy way to define piecewise functions; in *Derive*, linear combination of indicator functions can be used. Nspire CAS integrates symbolically any piecewise continuous function – and returns, as expected, an everywhere continuous antiderivative – as long as this function is not multiplied by another expression. *Derive* knows how to integrate  $\text{sign}(ax + b)f(x)$  where  $f$  is an arbitrary function,  $a$  and  $b$  real numbers and “sign” stands for the signum function: this is why products of a piecewise function with any other expression can be integrated symbolically. This will be the first part of our talk.

In the second part of this talk, we will show some implementations that will allow Nspire CAS to integrate symbolically products of piecewise functions with expressions: the starting point was the discovery of a non-documented function of Nspire CAS. Examples of various operations between two piecewise functions will be presented. As a final example, we will show how we have defined a Fourier series function in Nspire CAS that performs as well as *Derive*'s built-in “Fourier” function.

## Keywords

Piecewise functions, integration, Fourier series.

# A Toolbox with DERIVE: Calculus on Several Variables

Alfonsa García, Francisco García  
Technical University of Madrid (Spain)

Ángel Martín del Rey, Gerardo Rodríguez  
University of Salamanca (Spain)

Agustín de la Villa  
Technical University of Madrid & Pontificia Comillas University (Spain)

`avilla@upcomillas.es`

## Abstract

A toolbox is a set of procedures taking advantage of the computing power and graphical capacities of a CAS. With these procedures the students can solve math problems, apply mathematics to engineering or simply reinforce the learning of certain mathematical concepts.

From the point of view of their construction, we can consider two types of toolboxes:

- (i) the closed box, built by the teacher, in which the utility files are provided to the students together with the respective tutorials and several worksheets with proposed exercises and problems,
- (ii) the open box, in which the students are free to construct, under teacher's direction, their own toolbox, which the procedures useful for solving some problems.

Both models have pedagogical advantages and disadvantages. The ideal model will probably be a transition from the closed model, appropriate in the first year of engineering studies, to the open box model, useful for advanced mathematical topics.

The authors have experience in building both boxes using different CAS. This paper presents a closed box model, made with DERIVE, with procedures relating to the contents of a course in differential calculus of several variables. In the experiment, carried out during the 2012–2013 academic year at the Pontificia Comillas University, the students have received the toolbox. The students, working in a team, solved the problems proposed in the worksheets. They have delivered the files and they have completed a survey that attempts to measure the usefulness and satisfaction of the experience.

## Keywords

Toolboxes, Computer Algebra Systems, Engineering studies

# DERIVE and Linear Algebra

Alfonsa García, Francisco García  
Technical University of Madrid (Spain)

Ángel Martín del Rey, Gerardo Rodríguez  
University of Salamanca (Spain)

Agustín de la Villa  
Technical University of Madrid & Pontificia Comillas University (Spain)

`avilla@upcomillas.es`

## **Abstract**

This work describes an experience with a methodology for learning based on competences in Linear Algebra for engineering students. The experience has been based in autonomous team work of students.

DERIVE tutorials for Linear Algebra topics are provided to the students. They have to work with the tutorials as their homework. After, worksheets with exercises have been prepared to be solved by the students organized in teams, using DERIVE function previously defined in the tutorials. The students send to the instructor the solution of the proposed exercises and they fill a survey with their impressions about the following items: ease of use of the files, usefulness of the tutorials for understanding the mathematical topics and the time spent in the experience. As a final work, we have designed an activity directed to the interested students. They have to prepare a project, related with a real problem in Science and Engineering. The students are free to choose the topic and to develop it but they have to use DERIVE in the solution. Obviously they are guided by the instructor.

Some examples of activities related with Orthogonal Transformations will be presented.

## **Keywords**

Linear Algebra, Orthogonal Transformations, Team work, Computer Algebra Systems



# A Dynamic Unity of Tradition and Technology in Undergraduate Mathematics - a Bulgarian Experience

Elena A.Varbanova  
Technical University of Sofia (Bulgaria)

elvar@tu-sofia.bg

## Abstract

An overview of the author's experience in incorporating computer algebra into undergraduate mathematics education is represented. The paper focuses on the need for careful planning and informed use of computer algebra to achieve specific goals and objectives. A number of examples are considered showing how the CAS Derive is used as a symbolic, numeric and graphic instrument throughout the teaching-learning-assessment process in order to

- challenge existing ideas
- extend existing ideas
- work smarter not harder
- innovate not to imitate
- facilitate problem solving and save time
- make additional activities possible
- assess student's achievements.

By combined methodology in a CAS-supported environment it occurs that Tradition welcomes Technology and Technology salutes Tradition. The experience shows that appropriately created and structured activities integrated into the study plans have the potential to contribute to enhancement of the teaching and learning of mathematics.

## Keywords

Undergraduate mathematics, Tradition, Technology, CAS DERIVE



---

---

# Session 8: Computer Algebra in Algebraic Statistics

---

---

Organizers:

Hugo Maruri-Aguilar  
Eduardo Sáenz-de-Cabezón  
Henry P. Wynn



# Computing real log canonical thresholds in algebraic statistics

Hamid Ahmadinezhad, Josef Schicho  
RICAM, Austria

Caroline Uhler  
IST, Austria

`hamid.ahmadinezhad@oeaw.ac.at`

## Abstract

The real log canonical threshold (RLCT) is a numerical invariant that measures the complexity of a real singularity of an algebraic (or analytic) variety. It has appeared in algebraic geometry, differential geometry and more recently in algebraic statistics. We present different methods to compute the RLCT associated to directed Gaussian graphical models in causal inference. The RLCT plays an important role for causal inference since it allows the quantification of biases. So far, the RLCT could only be computed for some special small graphs and computations for larger graphs or classes of graphs remained open. We present new results related to the computation of the RLCT, give specific examples and also discuss the challenges related to such computations.

## Keywords

Real log canonical threshold, real singularity, blow up, Newton polyhedron, causal inference, bias quantification, directed Gaussian graphical model, collider-stratification bias

## 1 Introduction

Determining causal relations between variables is a fundamental goal in many areas of science. A popular approach is to model the causal relationships by a directed acyclic graph (DAG) and assume that the variables follow a Gaussian distribution. In various applications, it is of particular interest to estimate the edge weight of a particular edge  $E \rightarrow D$ , as for example the direct effect of an exposure  $E$  on a disease outcome  $D$  in the medical setting. The presence of multi-edge paths between the nodes  $E$  and  $D$  lead to bias in effect estimation (see e.g. [4, 5]). In a recent paper, Lin, Uhler, Sturmfels and Bühlmann [6] showed that quantifying such bias is related to the real log canonical threshold (RLCT) of a certain variety whose defining polynomial is a weighted sum over certain paths between  $E$  and  $D$ . In this paper, we first introduce directed Gaussian graphical models (Section 2) and a specific form of bias, namely collider-stratification bias (Section 3). We then introduce the RLCT and present some methods for computing the RLCT (Section 4). Then, we apply these methods to quantify collider-stratification bias in effect estimation for special classes of DAGs.

## 2 Directed Gaussian graphical models

The model considered in this paper is defined as follows: Let  $G = (V, E)$  be a weighted DAG with  $V = \{1, 2, \dots, p\}$ . Directed edges are denoted by  $i \rightarrow j$  or  $(i, j)$ . Without loss of generality we can assume that the vertices are topologically ordered, meaning that there can only be a directed edge  $i \rightarrow j$  if  $i < j$ . Then the edge weights (i.e. the direct causal effects) in a DAG  $G$  are given by a (strictly upper triangular) adjacency matrix  $A_G$  with entries  $a_{ij} \neq 0$  if  $(i, j) \in E$  and zero otherwise. To each node  $i$  we associate a random variable  $X_i$ . Defining a Gaussian graphical model by the linear structural equations  $X = A_G^T X + \epsilon$ , where  $X = (X_1, \dots, X_p)^T$  and  $\epsilon \sim \mathcal{N}(0, I)$ , the random vector  $X$  follows a Gaussian distribution with mean zero and inverse covariance matrix  $K = (A_G - I)(A_G - I)^T$ .

A particular edge weight  $a_{ij}$  is estimated from the partial correlation  $\text{corr}(i, j | S)$ , where  $S \subset V \setminus \{i, j\}$ . Algebraically, partial correlations can be computed from minors of the inverse covariance matrix  $K$  as follows:

$$\text{corr}(i, j | S) = \frac{\det(K_{iR, jR})}{\sqrt{\det(K_{iR, iR}) \cdot \det(K_{jR, jR})}}. \quad (1)$$

where  $R = V \setminus (S \cup \{i, j\})$  and  $iR = \{i\} \cup R$ . Since the denominator is always positive and only used for normalization to ensure that  $-1 \leq \text{corr}(i, j | S) \leq 1$ , we here concentrate on the numerator. To give a combinatorial description of  $\det(K_{iR, jR})$  based on paths in the DAG  $G$  the following graph-theoretic notions are needed: A node  $i$  is an ancestor of  $j$  if there is a directed path  $i \rightarrow \dots \rightarrow j$ , and a configuration  $i \rightarrow k, j \rightarrow k$  is called a *collider* at  $k$ . It was shown in [7, Equation (11)] that, combinatorially, the numerator  $\det(K_{iR, jR})$  is a linear combination of the weights of all *active* paths between  $i$  and  $j$  given  $S$ , meaning all undirected paths  $P$  between  $i$  and  $j$  such that every non-collider in  $P$  is not in  $S$  and every collider in  $P$  is in  $S$  or an ancestor of a node in  $S$ . For estimating the direct effect  $a_{ij}$  from  $\text{corr}(i, j | S)$ , all active paths other than the direct edge are thus considered as bias.

The volume of the “tube” corresponding to  $\text{corr}(i, j | S)$ ,

$$\text{Tube}_{i, j | S}(\lambda) = \{ (a_{ij})_{(i, j) \in E} \in \mathbb{R}^{|E|} : |\text{corr}(i, j | S)| \leq \lambda \}, \quad (2)$$

in a DAG where the edge  $(i, j)$  has been removed, is of particular interest for quantifying the bias when estimating the direct effect  $a_{ij}$ . For  $\lambda$  close to zero, this tube corresponds to the parameters which contribute negligibly to the bias. So the larger the volume

$$V_{i, j | S}(\lambda) = \int_{\text{Tube}_{i, j | S}(\lambda)} \varphi(\omega) d\omega \quad (3)$$

(where  $\varphi$  is taken to be the Lebesgue measure), the smaller the bias in effect estimation. For small values of  $\lambda$  it has been shown in [6] that

$$V_{i, j | S}(\lambda) \approx C \cdot \lambda^l \cdot (-\ln \lambda)^{m-1},$$

where  $C$  is a positive constant,  $l \in \mathbb{Q}_+$  and  $m \in \mathbb{Z}_+$ .

**Definition 2.1.** The *real log canonical threshold* (RLCT) of the hypersurface corresponding to the vanishing of the polynomial  $f = \text{corr}(i, j | S)$ , or equivalently to  $\det(K_{iR, jR}) = 0$ , with respect to a measure  $\varphi(x) dx$  at  $\Omega$ , is defined as

$$\text{RLCT}_{\Omega}(f, \varphi) = (\ell, m).$$

RLCTs are ordered reversely by the size of  $\lambda^{\ell} (-\ln \lambda)^{m-1}$ , i.e.

$$(\ell_1, m_1) < (\ell_2, m_2) \iff \ell_1 < \ell_2 \text{ or } \ell_1 = \ell_2 \text{ and } m_1 > m_2.$$

In Section 4, we study the RLCT in more detail and show how to compute it in specific examples of relevance to bias quantification in causal inference.

### 3 Collider-stratification bias

In this paper, we focus on a particular form of bias, namely *collider-stratification bias*. Suppose we are given a DAG  $G$  with  $i, j \in V$  and there is another node  $C$  such that

$$i \rightarrow V_1 \rightarrow \dots \rightarrow V_s \rightarrow C \leftarrow W_1 \leftarrow \dots \leftarrow W_t \leftarrow j.$$

Stratifying (i.e. conditioning) on  $C$  activates the above path between  $i$  and  $j$  leading to bias when estimating  $a_{ij}$ . The partial correlation corresponding to this active path between  $i$  and  $j$  is known as *collider-stratification bias*.

It is widely believed that collider-stratification bias tends to attenuate when it arises from more extended paths (see [3, 4] and Problem 6.2 in [6] for a precise mathematical conjecture). In the following, we give further evidence for this conjecture based on computations for a specific class of DAGs, namely *complete tripartite graphs*, DAGs consisting of three “levels” of vertices,  $A = \{1, 2\}$ ,  $B = \{1, 2, \dots, m\}$  and  $C = \{1, 2, \dots, n\}$ , where  $(a, b) \in E$  and  $(b, c) \in E$  for all  $a \in A$ ,  $b \in B$  and  $c \in C$ . An example is shown in Figure 1.

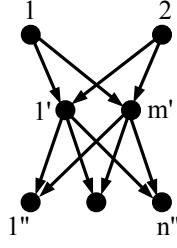


Figure 1: Complete tripartite graph.

For complete tripartite graphs the conjecture regarding the attenuation of bias over long paths can be formulated as follows (see also Problem 6.2 in [6]):

$$V_{1,2|B}(\lambda) \leq V_{1,2|C}(\lambda), \quad (4)$$

meaning that the bias introduced when conditioning on the nodes in  $B$  is larger than when conditioning on the nodes in  $C$ . This conjecture has been proven when  $m = 1$  [6, Example 6.3] or  $n = 1$  [6, Example 6.5]. We therefore concentrate on  $m, n > 1$ .

To prove this conjecture, we need to compute the RLCT corresponding to the two hypersurfaces defined by  $K_{1C,2C}$  and  $K_{1B,2B}$ . We first describe these two polynomials in terms of paths in the DAG. For simplicity of notation, we denote the edge weights between nodes in  $A$  and  $B$  by  $a_{ij}$  and the edge weights between nodes in  $B$  and  $C$  by  $b_{ij}$ .

The path representation of  $K_{1C,2C}$  when conditioning on  $B$  is simple. It is just the sum over all paths going from node 1 to some node in  $B$  to node 2, i.e.

$$K_{1C,2C} = \sum_{s=1}^m a_{1s} a_{2s}. \quad (5)$$

Finding a path representation for  $K_{1B,2B}$  when conditioning on  $C$  is more difficult, but can be done by applying the explanations in [7, Section 4]. For space reasons we here only give the formula when either  $|B| = 2$  or  $|C| = 2$ . For  $|B| = 2$

$$K_{1B,2B} = \sum_{s=1}^2 a_{1s} a_{2s} \left[ \sum_{i=1}^n b_{si}^2 \left( 1 + \sum_{j \neq i, t \neq s} b_{tj}^2 \right) - 2 \sum_{i \neq j} b_{1i} b_{1j} b_{2i} b_{2j} \right] + \sum_{s \neq t} a_{1s} a_{2t} \sum_{i=1}^n b_{1i} b_{2i}.$$

This formula consists of two main components, paths which go from the two nodes in  $A$  to the same node  $s \in B$ , and paths which go to different nodes  $s, t \in B$ . For the paths which go to the same node  $s \in B$ , there are two possibilities: either

$$1 \rightarrow s \rightarrow i \leftarrow s \leftarrow 2, \quad \text{where } s \in B, i \in C$$

and this can be multiplied with cycles of length 2 in the remaining nodes, or

$$1 \rightarrow s \rightarrow i \leftarrow t \rightarrow j \leftarrow s \leftarrow 2, \quad \text{where } s \neq t \in B, i \neq j \in C.$$

The paths which go to different nodes  $s, t \in B$  then need to find together in  $C$  and hence are of the form

$$1 \rightarrow s \rightarrow i \leftarrow t \leftarrow 2, \quad \text{where } s \neq t \in B, i \in C.$$

For  $|C| = 2$  the path representation is slightly more complicated, but follows along the same lines as for  $|B| = 2$ :

$$K_{1B,2B} = \sum_{s=1}^m a_{1s} a_{2s} \left[ \sum_{i=1}^2 b_{si}^2 \left( 1 + \sum_{t \neq s, j \neq i} b_{tj}^2 \right) - 2 b_{s1} b_{s2} \sum_{t \neq s} b_{t1} b_{t2} \right] + \sum_{s \neq t} a_{1s} a_{2t} \left[ \sum_{i=1}^n b_{si} b_{ti} \left( 1 + \sum_{r \neq s, t, j \neq i} b_{rj}^2 \right) - \sum_{i \neq j} b_{si} b_{tj} \left( \sum_{r \neq s, t} b_{ri} b_{rj} \right) \right].$$

In the following section we describe some methods to compute the RLCTs corresponding to  $K_{1B,2B}$  and  $K_{1C,2C}$ . This will provide a big step towards the proof of the conjecture in general, while completes the proofs for some specific complete tripartite graphs.

## 4 Real log canonical threshold

In the following, we recall two methods to compute the RLCT and explain how they can be applied to compute the relevant RLCTs in the conjecture discussed in the previous section.

### Method I: Blow up.

The following proposition, which was proven in [6], shows how a change of variables or a blow up effects the RLCT.

**Proposition 4.1** ([6], Proposition 3.5). Suppose  $\varphi(\omega) = \omega_1^{\tau_1} \dots \omega_d^{\tau_d}$  and  $f(\omega) = \omega_1^{\kappa_1} \dots \omega_r^{\kappa_r} g(\omega)$ , where  $\kappa_1, \dots, \kappa_r$  are nonzero and the hypersurface  $\{g(\omega) = 0\}$  is normal crossing with  $\omega_1, \dots, \omega_r$ . Let  $\omega_0$  denote the function  $g$  and let  $\kappa_0 = 1, \tau_0 = 0$ . Define

$$l = \min_{i \in \mathcal{I}} \frac{\tau_i + 1}{\kappa_i}, \quad \mathcal{J} = \operatorname{argmin}_{i \in \mathcal{I}} \frac{\tau_i + 1}{\kappa_i}, \quad m = |\mathcal{I}|,$$

where  $\mathcal{I}$  is the set of all indices  $0 \leq i \leq r$  such that  $\omega_i$  has a root in  $\Omega$ . If the equations  $\omega_i = 0$  for  $i \in \mathcal{J}$  has a root in the interior of  $\Omega$ , then  $\operatorname{RLCT}_{\Omega}(f; \varphi) = (l, m)$ .

Applying this method we can compute the RLCT of the polynomial  $K_{1C,2C}$  given in (5). Note that this polynomial only consists of paths between nodes in  $A$  and in  $B$  and hence only depends on  $|B| = m$ :

**Lemma 4.2.**  $\operatorname{RLCT}(K_{1C,2C}) = \begin{cases} (1, 2) & \text{if } m = 1 \\ (1, 1) & \text{if } m \geq 2 \end{cases}$

*Proof.* For brevity, we denote  $K_{1C,2C}$  by  $f$ . We recall that a point  $p$  of a hypersurface is *singular* if all first order partial derivatives vanish at this point. Note that  $f$  is singular only at the origin. Blowing up the hypersurface  $\{f = 0\}$  at the origin leads to a new variety  $Y$ , which is birational to  $X$ . It is defined by

$$u^2 f = 0 \subset \mathbb{R}P^{2m-1} \times \mathbb{R},$$

where the coordinates on  $\mathbb{P}_{\mathbb{R}}^{2m-1}$  are  $a_{11}, \dots, a_{1m}, a_{21}, \dots, a_{2m}$ , and  $u$  is the coordinate on  $\mathbb{R}$ . It is covered by  $2m$  patches. The first patch, for example, is defined by

$$\{u^2(a_{21} + a_{12}a_{22} + \dots + a_{1m}a_{2m}) = 0\} \subset \mathbb{R}^{2m}$$

The contribution of the Jacobian gives  $\varphi = u^{2m-1}$ . One can then easily check that the RLCT at this patch is  $(1, 1)$  using Proposition 4.1. The claim follows as the computation on all patches are identical.  $\square$

### Method II: Newton Polyhedron.

Let  $f = \sum \mathcal{M}_i$  be a polynomial in  $n$  variables  $x_1, \dots, x_n$ , where  $\mathcal{M}_i = c_i x_1^{m_{i1}} \dots x_n^{m_{in}}$  are the monomials appearing in  $f$  with  $c_i \neq 0$ . The *Newton polyhedron* of  $f$  is denoted by  $\mathcal{P}(f)$  and is defined as the convex hull generated by  $(m_{i1}, \dots, m_{in}) \in \mathbb{R}^n$  for  $i = 1, \dots, r$ . For a compact subset  $\mathcal{C} \subset \mathbb{R}^n$  the corresponding *face polynomial* is given by

$$f_{\mathcal{C}} = \sum_{i: (m_{i1}, \dots, m_{in}) \in \mathcal{C}} \mathcal{M}_i.$$

A polynomial  $f$  is *nondegenerate* if all face polynomials are non-singular in  $(\mathbb{R}^*)^n$ . i.e.

$$\operatorname{Sing}(f_{\mathcal{C}}) \cap (\mathbb{R}^*)^n = \emptyset \quad \text{for all compact faces } \mathcal{C} \subset \mathcal{P}(f).$$

Then for a polynomial  $f$  the real log canonical threshold of its Newton polyhedron is defined as

$$\operatorname{RLCT}(\mathcal{P}(f)) = (\tau, \theta),$$

where  $\tau = \sup\{r \mid \mathbf{1} \notin r\mathcal{P}(f)\}$  and  $\theta$  is the codimension of the face of  $\tau\mathcal{P}(f)$  that contains  $\mathbf{1}$ .

The following result from [2] gives a sufficient condition for equality of the RLCT of a polynomial and the RLCT of its Newton polyhedron.



**Theorem 4.3** ([2], §8.3). *If  $f$  is non-degenerate and has a minimum or maximum near the origin then  $\text{RLCT}(f) = \text{RLCT}(\mathcal{P}(f))$ .*

In the following theorem we show that the unnatural and non-algebraic condition of having a minimum or maximum close to the origin can in fact be removed:

**Theorem 4.4.** *If  $f$  is non-degenerate then  $\text{RLCT}(f) = \text{RLCT}(\mathcal{P}(f))$ .*

*Sketch of the proof.* The condition of having a minimum or maximum close to the origin in the proof of Theorem 4.3 guarantees that  $\text{Sing}(f)$  contains real points. However, one can verify that this statement follows directly from the non-degeneracy of  $f$ . For a complete proof see the forthcoming extended version of this paper.  $\square$

In the following we describe work in progress. Our conjecture is that the polynomial  $K_{1B,2B}$  is non-degenerate for all sizes  $m = |B|$  and  $n = |C|$ . One can check this conjecture for small values of  $m, n$  using the `Macaulay2` library `asymptotics.m2`, and we are working on a general proof. It then follows from Theorem 4.4 that the  $\text{RLCT}$  of  $K_{1B,2B}$  equals the  $\text{RLCT}$  of its Newton polyhedron. For small examples of  $m, n > 1$  one can check using methods of Lin [1] in `Macaulay2` by computing the  $\text{RLCT}$  of the Newton polyhedron that  $\text{RLCT}(\mathcal{P}(K_{1B,2B})) = (1, 1)$ . We are working on proving this conjecture for general  $m, n > 1$ . As a consequence one would get

$$\text{RLCT}(\mathcal{P}(K_{1C,2C})) = (1, 1) = \text{RLCT}(\mathcal{P}(K_{1B,2B})).$$

So in order to prove the general conjecture  $V_{1,2|B}(\lambda) \leq V_{1,2|C}(\lambda)$  for small  $\lambda > 0$ , we need to analyze the constants.

The examples considered in this paper indicate that only computing the  $\text{RLCT}$  is often not sufficient for answering questions of interest in causal inference. This has been noted also in [6] and some results regarding the computation of the constants has appeared in [6, Chapter 8]. However, in order to solve some of the important problems related to the quantification of bias in causal inference, further research in this direction is necessary.

## References

- [1] Shaowei Lin, *Asymptotic Approximation of Marginal Likelihood Integrals*. arXiv:1003.5338, 2010.
- [2] V. I. Arnold, S. M. Gusein-Zade and A. N. Varchenko, *Singularities of Differentiable Maps*. Vol. II, Birkhäuser, Boston, 1985.
- [3] S. Chaudhuri and T.S. Richardson: Using the structure of d-connecting paths as a qualitative measure of the strength of dependence, *Proceedings of the Nineteenth Conference on Uncertainty in Artificial Intelligence*, pages 116–123, 2003.
- [4] S. Greenland: Quantifying biases in causal models: classical confounding vs collider-stratification bias, *Epidemiology* **25**, pages 300–306, 2003.
- [5] S. Greenland and J. Pearl: Adjustments and their consequences: collapsibility analysis using graphical models, *International Statistical Review* **79**, pages 401–426, 2011.
- [6] S. Lin, C. Uhler, B. Sturmfels, P. Bühlmann, *Hypersurfaces and their singularities in partial correlation testing*. arXiv:1209.0285, 2012.
- [7] C. Uhler, G. Raskutti, B. Yu and P. Bühlmann, *Geometry of faithfulness assumption in causal inference*, arXiv:1207.0547, 2012.

# Error evaluation for algebraic interpolatory cubature formulæ

Claudia Fassino, Eva Riccomagno  
University of Genova (Italy)

fassino@dima.unige.it

## Abstract

In this work we remark on the error estimation in cubature formulae. We combine methods from Commutative Computational Algebra and Orthogonal Polynomial Theory to address a problem common to many disciplines: the estimation of the expected value of a polynomial of a random vector using a linear combination of a finite number of its values.

## Keywords

Design of experiments, Interpolatory cubature formulæ, Expected values, Orthogonal polynomials, Gröbner bases

## 1 Introduction

We continue work in [1] which addresses the classical cubature problem with tools from Algebraic Statistics for experimental design ([6, 7]) and Computational Commutative Algebra. Related seminal work is in ([5, 4]). We deal with the classical problem of computing the expected value of a real function  $f$  of the  $d$ -variate random vector  $X$  as a linear combination of its values  $f(z)$  at a finite set of points  $z \in \mathcal{D} \subset \mathbb{R}^d$ .

Fassino et al. (2013) in [1] consider the computational algebra setting for the problem of approximating the expected value of multidimensional polynomial functions by means of cubature formulæ. All functions and quantities intervening in their computations are expressed in terms of a given set of orthogonal polynomials. A good reference for orthogonal polynomials is [2]. In particular we reformulate Theorem 7 in [1] in order to characterize the error of a cubature rule and generalize it to non-product probability measures.

## 2 The error formula

Let  $\mathcal{D} \subset \mathbb{R}^d$  be a finite set of distinct real points in  $d$ -dimension,  $\mathcal{D} \subset \mathbb{R}^d$  and  $\mathbb{R}[x]$  with  $x = (x_1, \dots, x_d)$  the set of polynomials with real coefficients in  $d$  indeterminates. We fix a term ordering  $\sigma$  on  $\mathbb{R}[x]$ . In the examples we use the degree lexicographic term ordering with  $x_2 < x_1$ . Let  $\mathcal{I}(\mathcal{D})$  be the vanishing ideal of  $\mathcal{D}$  and  $G$  the  $\sigma$ -reduced Gröbner basis of  $\mathcal{I}(\mathcal{D})$ .

**Example 1** For the five point design in two dimensions

$$\mathcal{D} = \{(x_1, x_2) \in \mathbb{R}^2 : x_1^3 - 3x_1 = x_2^3 - 3x_2 = x_1^2 - x_2^2 = 0\},$$

the  $\sigma$ -reduced Gröbner basis,  $G$ , of the vanishing ideal of  $\mathcal{D}$ ,  $\mathcal{I}(\mathcal{D})$ , is  $g_1 = x_1^2 - x_2^2$ ,  $g_2 = x_2^3 - 3x_2$ ,  $g_3 = x_1x_2^2 - 3x_1$ .

By Euclidean division with respect to  $G$ , a polynomial  $p \in \mathbb{R}[x]$  can be written as

$$p = \sum_{g \in G} q_g g + r$$

where the remainder  $r$  is the unique element of  $\mathbb{R}[x]/\mathcal{I}(\mathcal{D})$  such that  $p(d) = r(d)$  for all  $d \in \mathcal{D}$  and no term of  $r$  is divisible by the leading terms of  $g \in G$ . Importantly  $r$  is a linear combination of the type  $r = \sum_{\alpha \in L} c_\alpha x^\alpha$  with  $L = L_{\sigma, \mathcal{D}} = \{\alpha \in \mathbb{Z}_{\geq 0}^d : x^\alpha \notin LT(\mathcal{I}(\mathcal{D}))\}$ . Here  $LT(p)$  is the leading term of  $p$  with respect to  $\sigma$ . The quotients  $q_g$ ,  $g \in G$ , do not need to be unique.

**Example 2** In the set-up of Example 1, for  $p = x_1^4 x_2^2 - 4x_1^4 - 6x_1^2 x_2^2 + 24x_1^2 + 3x_2^2 - 12$  we have  $q_{g_1} = x_1^2 x_2^2 + x_2^4 - 4x_1^2 - 10x_2^2 + 24$ ,  $q_{g_2} = x_2^3 - 7x_2$ ,  $q_{g_3} = 0$  and  $r = 6x_2^2 - 12$ .

We start with a particular class of orthogonal polynomials. Let  $\lambda$  be a one-dimensional probability measure with finite moments and  $\{\pi_n\}_{n \in \mathbb{Z}_{\geq 0}}$  be its associated orthogonal polynomial system. To a multi-index  $\alpha = (\alpha_1, \dots, \alpha_d) \in \mathbb{Z}_{\geq 0}^d$  we associate the monomial  $x^\alpha = x_1^{\alpha_1} \cdots x_d^{\alpha_d}$  and the product of polynomials  $\pi_\alpha(x) = \pi_{\alpha_1}(x_1) \cdots \pi_{\alpha_d}(x_d)$ . Note that  $\{\pi_\alpha\}_\alpha$  is a system of orthogonal polynomials for the product measure  $\lambda^{\otimes d}$  under stochastic independence.

A monomial  $x^\alpha$  of total degree  $s = \sum_{i=1}^d \alpha_i$  is a unique linear combination of  $\pi_\beta$  where  $\sum_{i=1}^d \beta_i \leq s$  and viceversa any  $\pi_\beta$  is a linear combination of  $x^\alpha$  with  $\sum_{i=1}^d \beta_i \geq \sum_{i=1}^d \alpha_i$ . Hence for any multi-index  $\alpha$  there are a monomial  $x^\alpha$  and an orthogonal polynomial  $\pi_\alpha$ . A term-ordering  $\sigma$  for the  $x^\alpha$  corresponds to an ordering for the  $\pi_\alpha$ .

**Example 3** As reference measure  $\lambda$  we take the standard normal distribution whose density is  $f(z) = \sqrt{2\pi}e^{-z^2/2}$ ,  $z \in \mathbb{R}$  and whose corresponding orthogonal polynomials are the Hermite polynomials, indicated with  $H_n(z)$ ,  $n = 0, 1, \dots$ . For example  $H_0(z) = 1$ ,  $H_1(z) = z$ ,  $H_2(z) = z^2 - 1$  and  $H_{(i,j)}(x_1, x_2) = H_i(x_1)H_j(x_2)$  for  $i, j = 0, 1, \dots$ . With this notation we can write the  $g$  polynomials in Example 1 as  $g_1 = H_2(x_1) - H_2(x_2)$ ,  $g_2 = H_3(x_2)$ ,  $g_3 = H_1(x_1)(H_2(x_2) - 2)$ .

**Theorem 1 (Theorem 9 in [1])** *With the notation above, for  $g \in G$  and  $x^\alpha = LT(g)$  write*

$$g = \pi_\alpha - \sum_{\alpha >_\sigma \beta \in L} c_\beta(g) \pi_\beta \quad (1)$$

where  $\alpha >_\sigma \beta \in L$  stands for  $\alpha >_\sigma \beta$  and  $\beta \in L$ . For  $p = \sum_{g \in G} q_g g + r \in \mathbb{R}[x]$  consider the Fourier expansion of each  $q_g = \sum_{\beta} c_\beta(q_g) \pi_\beta$  and the Fourier expansion of  $r = \sum_{\alpha \in L} c_\alpha(r) \pi_\alpha$ . Let  $X$  be a random vector following  $\lambda^d$ . Then

1.  $E_\lambda(p(X)) = E_\lambda(r(X)) + R_n(p)$  where  $n$  is the number of points in  $\mathcal{D}$  and

$$R_n(p) = \sum_{g \in G} \|\pi_\alpha\|_\lambda^2 c_\alpha(q_g) - \sum_{g \in G} \sum_{\alpha >_\sigma \beta \in L} \|\pi_\beta\|_\lambda^2 c_\beta(q_g) c_\beta(g), \quad (2)$$

2.  $E_\lambda(r(X)) = \sum_{z \in \mathcal{D}} p(z) E_\lambda(\lambda_z(X))$  where  $\lambda_z(x)$  is the indicator function of the point  $z \in \mathcal{D}$ :  $\lambda_z(x) = 1$  if  $x = z$  and  $\lambda_z(x) = 0$  if  $x \in \mathcal{D} \setminus \{z\}$  and

3. furthermore

$$E_\lambda(p(X)) = c_{0_d}(p) = c_{0_d}(r) + R_n(p)$$

where  $0_d$  is the  $d$ -dimensional vector with all components equal to zero.

Assume now a (possibly non-product) probability measures,  $\lambda$  admitting a system of orthogonal polynomials  $\{\pi_\alpha\}_\alpha$ ,  $\alpha \in \mathbb{Z}_{\geq 0}^d$ . Theorem 2 generalises Theorem 1 to such a measure. Item 2 has already been observed in [3].

**Theorem 2** *Let  $\lambda$  be a probability measure with a system of orthogonal polynomials,  $\{\pi_\alpha\}_\alpha$ . Let  $\mathcal{D} \in \mathbb{R}^d$  be a finite set of  $n$ -distinct points,  $\sigma$  a term ordering on  $\mathbb{R}[x]$  and  $G$  a  $\sigma$ -reduced Gröbner basis for  $\mathcal{I}(\mathcal{D})$ . Write  $p \in \mathbb{R}[x]$  as  $p = \sum_{g \in G} q_g g + r$  by Euclidean division. Consider the Fourier expansions of the following polynomials  $g = \sum_{\alpha} c_\alpha(g) \pi_\alpha$  for all  $g \in G$ , of  $q_g = \sum_{\beta} c_\beta(q_g) \pi_\beta$  for all  $g \in G$  and of  $r = \sum_{\gamma} c_\gamma(r) \pi_\gamma$ . Then*

1.  $E_\lambda(p(X)) = E_\lambda(r(X)) + R_n(p)$  and

$$R_n(p) = \sum_{g \in G} \sum_{\alpha} \|\pi_\alpha\|_\lambda^2 c_\alpha(q_g) c_\alpha(g) \quad (3)$$

and both sums are finite,

2.  $E_\lambda(r(X)) = \sum_{z \in \mathcal{D}} p(z) E_\lambda(\lambda_z(X))$  where  $\lambda_z(x)$  is the indicator function of  $z \in \mathcal{D}$  and

3. furthermore  $E_\lambda(p(X)) = c_{0_d}(p) = c_{0_d}(r) + R_n(p)$ .

**Proof.** The proof is similar to that of Theorem 1 which relies on general properties of orthogonal polynomials, on polynomial division and on rearranging terms of Fourier expansions. By linearity of expectation from

$$p(x) = \sum_{g \in G} q_g g + r = \sum_{g \in G} q_g g + \sum_{z \in \mathcal{D}} p(z) \lambda_z$$

we deduce

$$E_\lambda(p(X)) = \sum_{g \in G} E_\lambda(q_g(X)g(X)) + \sum_{z \in \mathcal{D}} p(z) E_\lambda(\lambda_z(X)).$$

Substitute the Fourier expansions in the first sum

$$\sum_{g \in G} q_g g = \sum_{g \in G} \left( \sum_{\beta} c_\beta(q_g) \pi_\beta \sum_{\alpha} c_\alpha(g) \pi_\alpha \right)$$

These are all finite sums because Fourier expansions of polynomials and because  $G$  is finite. Expectation of  $\pi_\alpha(X)\pi_\beta(X)$  with  $\alpha \neq \beta$  is zero because of orthogonality:  $E_\lambda(\pi_\alpha(X)\pi_\beta(X)) = 0$  if  $\alpha \neq \beta$  and if  $\alpha = \beta$  it is equal to the square norm  $\|\pi_\alpha\|_\lambda^2$ . Thus taking expectation of (2) gives

$$E_\lambda \left( \sum_{g \in G} q_g(X)g(X) \right) = \sum_{g \in G} \sum_{\alpha} \|\pi_\alpha\|_\lambda^2 c_\alpha(q_g) c_\alpha(g).$$

Item 2 and 3 can be proven as in Theorem 1. ◇

Theorems 1 and 2 give necessary and sufficient conditions for exact quadrature of any polynomial  $p \in \mathbb{R}[x]$ . They also give a formula for the error. Item 3 follows by applying  $E_\lambda(\pi_\alpha(X)) = 0$  for all  $\alpha \in \mathbb{Z}_{\geq 0}^d \setminus \{0_d\}$  to the Fourier expansions of  $p$  and  $r$ . Item 2 gives the cubature formula expressed in terms of the values of  $p$  at the points in  $\mathcal{D}$  and in terms of  $\mathcal{D}$ . The weights of the cubature rule  $E_\lambda(\lambda_z(X))$  depend on the polynomial indicator functions  $\lambda_z(x)$  of  $z \in \mathcal{D}$ .

As the algebraic variety  $\mathcal{D}$  is zero-dimensional, all quantities involved in Theorem 1 can be computed with linear operations. Table 4 in [1] gives the relationship between the Gröbner basis of  $\mathcal{D}$  and the orthogonal polynomials (see (iii) in [3]). It provides an analogue of the Buchberger-Möller (O-BM) algorithm for orthogonal polynomials and it computes a  $\sigma$ -reduced Gröbner basis of  $\mathcal{I}(\mathcal{D})$  by working only in the space of orthogonal polynomials. A by-product of the O-BM algorithm is the computation of the Fourier coefficients of  $r$ . In particular it returns  $c_{0_d}(r)$  in Item 3, that is the value of the cubature rule giving the estimation of the expected value of  $p(X)$  and the exact value of  $E_\lambda(r(X))$ . For Theorem 2 we are not able to make analogue statements yet.

### 3 Remarks on the error formula

- The expected values of polynomials of “low degree” is the value of the cubature rule and the error is zero. Indeed consider  $p = \sum_{\alpha \in L} c_\alpha x^\alpha \in \mathbb{R}[x]/\mathcal{I}(\mathcal{D})$  where  $L = L_{\sigma, \mathcal{D}}$  depends only on the Gröbner basis  $G$  and hence only on the design and the term ordering. Then the quotients  $q_g$  of the Euclidean division of  $p$  by  $G$  are all zero and the error formulæ (2) and (3) are zero. In particular all moments  $E_\lambda(X^\alpha)$  with  $\alpha \in L$  are zero (see also [3]).
- The error formulæ (2) and (3) are linear polynomials in the Fourier coefficients  $c_\alpha(q_g)$  which determine the polynomial  $p$ . Whilst the norms of the orthogonal polynomials  $\pi_\alpha$  are supposed known and the Fourier coefficients  $c_\alpha(g)$  are derived from the design  $\mathcal{D}$  and the term ordering  $\sigma$ . For the case of product probability measure they can be computed by the algorithm in Table 4 in [1].
- The error formula (3) can be seen as the scalar product of two vectors. The sum over  $\alpha$  is finite and goes up to the largest leading term of  $g \in G$ . Let

$$T_G = \bigcup_{g \in G} \left\{ \alpha \in \mathbb{Z}_{\geq 0}^d : c_\alpha(g) \neq 0 \text{ with } g = \sum_{\alpha} c_\alpha(g) \pi_\alpha \right\}$$

Fix  $\alpha \in T_G$  then each term in the error formula (3) is the scalar product of the two vectors  $(c_\alpha(q_g) : g \in G)$  and  $(c_\alpha(g) : g \in G)$ , call it  $s_\alpha$ . Then we can define a weighted relative cubature error as  $S_n(p) = \frac{R_n(p)}{\sum_{\alpha \in T_G} \|\pi_\alpha\|^2} = \frac{\sum_{\alpha \in T_G} s_\alpha(p) \|\pi_\alpha\|^2}{\sum_{\alpha \in T_G} \|\pi_\alpha\|^2}$ .

- It is known that the quotients of division are not necessarily unique even when dividing by a reduced Gröbner basis. This does not have an effect on the value of error  $R_n(p)$  as the error in the cubature rule is unique. A simple algebraic proof is: for the  $\sigma$ -reduced Gröbner basis of  $\mathcal{I}(\mathcal{D})$ ,  $G$ , and  $p$  a polynomial, consider two results of the Euclidean division of  $p$  by  $G$

$$p = \sum_{g \in G} q_g g + r = \sum_{g \in G} q'_g g + r$$

where the remainder is the same and  $q_g$  and  $q'_g$  could be different. Taking expectation gives

$$R_n(p) = \sum_{g \in G} \sum_{\alpha} \|\pi_\alpha\|_\lambda^2 c_\alpha(q_g) c_\alpha(g) = \sum_{g \in G} \sum_{\alpha} \|\pi_\alpha\|_\lambda^2 c_\alpha(q'_g) c_\alpha(g).$$

- If  $G$  is a  $\sigma$ -reduced Gröbner basis and for each  $g \in G$  there exists  $\gamma$  such that  $g = \pi_\gamma$  then  $R_n(p)$  in (3) simplifies to  $R_n(p) = \sum_{\gamma} \|\pi_\gamma\|_\lambda^2 c_\gamma(q_\gamma)$ . Next we show some particular cases.
- Consider the particular case of product grid, that is the design  $\mathcal{D}$  is a product grid of zeros of univariate orthogonal polynomials:

$$\mathcal{D} = \{x = (x_1, \dots, x_d) \in \mathbb{R}^d : \pi_{n_i}(x_i) = 0 \text{ with } n_i \in \mathbb{Z}_{>0} \text{ and } i = 1, \dots, d\}.$$

This implies a product probability measure. Then  $G = \{\pi_{n_1}(x_1), \dots, \pi_{n_d}(x_d)\}$ , the second term in Formula (2) is zero for every polynomial  $p$  and the error simplifies to  $R_n(p) = \sum_{i=1}^d \|\pi_{n_i}\|_\lambda^2 c_{n_i}(q_i)$ .

Furthermore  $c_{n_i}(q_i) = 0$  if  $p$  does not include the term  $x_i^{2n_i}$ . It follows that the cubature rule is exact for all polynomials  $p$  such that for all  $i = 1, \dots, d$  their degree in the variables  $x_i$  is smaller than  $2n_i$ . Recall that  $n_i$  is the number of distinct zeros of  $\pi_{n_i}(x_i)$ . This is a high-dimensional analogue of the well-known result for one-dimensional quadrature rules stating that they are exact for all polynomials of degree at most  $2n - 1$  where  $n$  is the number of nodes.

We conclude with our running example.

**Example 4** To compute the value of cubature rule we use the algorithm in Table 4 in [1] and find that  $E_\lambda(r(X)) = -6$ . To estimate the error  $R_n(p)$  we compute the Fourier expansions of  $q_{g_i}$ ,  $i = 1, 2, 3$  by hand by using Theorem 4 in [1] and obtain

$$q_{g_1} = H_4(x_1)H_4(x_2) + 6H_2(x_1)H_4(x_2) - H_4(x_1) + 3H_4(x_2), \quad q_{g_2} = H_3(x_2) - 4H_1(x_2), \quad q_{g_3} = 0.$$

From this we deduce that  $g_1$  and  $g_3$  contribute zero to  $R_n(p)$  in Formula (2) and

$$R_n(p) = \|H_3(x_2)\|_\lambda^2 c_{(0,3)}(q_{g_2}) = 3!1 = 6.$$

In this case we can check directly that indeed  $E_\lambda(p(X)) = 0$ .

Notice that in the application we have in mind, a typical one in numerical integration, we do not know  $p$  (only the values of  $p$  at  $\mathcal{D}$  are available) and hence we cannot know the  $q_{g_i}$ . It would be interesting to use error formulæ (2) and (3) to determine larger classes of  $\mathcal{D}$  and  $p$  for which the cubature rule is exact than the product grid we give above.

## References

- [1] C. Fassino, G. Pistone and E. Riccomagno (2013). The algebra of interpolatory cubature formulæ for generic nodes. Statistics and Computing DOI 10.1007/s11222-013-9392-6 (in press)
- [2] W. Gautschi (2004). Orthogonal polynomials: computation and approximation. Oxford University Press, New York.

- [3] J. Ko and H.P. Wynn (2013). Quadrature rules for polynomial chaos expansion using the algebraic method in the design of experiments. In Book of Abstracts of Seventh International-Workshop on Simulation (M. Matteucci ed.) 371-372.
- [4] H. M. Möller (1987). On the construction of cubature formulae with few nodes using Groebner bases. Numerical integration (Halifax, N.S., 1986), NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., vol. 203, Reidel, Dordrecht, 1987, pp. 177-192.
- [5] H. M. Möller and B. Buchberger (1982). The construction of multivariate polynomials with preassigned zeros. In Computer algebra (Marseille, 1982), Lecture Notes in Comput. Sci., Springer, Berlin, 144, 24–31.
- [6] G. Pistone, E. Riccomagno and H. P. Wynn (2001). Algebraic statistics. Chapman & Hall/CRC, Boca Raton, FL.
- [7] E. Riccomagno (2009). A brief history of algebraic statistics. *Metrika* 69, 397–418.

# A Gröbner Bases Method for Complementary Sequences

Christos Koukouvinos

National Technical University of Athens, Greece

Dimitris E. Simos\*

SBA Research, 1040 Vienna, Austria

Zafeirakis Zafeirakopoulos†

RISC - Research Institute for Symbolic Computation, Linz, Austria

zafeirakopoulos@risc.jku.at

## Abstract

We employ tools from the field of symbolic computation for the construction of new classes of combinatorial designs, in particular complementary sequences and orthogonal designs. Combinatorial designs are used in a variety of applications ranging from statistics to coding theory and from telecommunications to software testing.

## Keywords

Complementary Sequences, Orthogonal Designs, Gröbner Bases, Algebraic Modeling

## 1 Introduction

Orthogonal designs (ODs) are square matrices with entries in the field of quotients of the integral domain  $\mathbb{Z}[a_1, a_2, \dots, a_\ell]$  with certain orthogonality properties while complementary sequences are tuples of sequences with zero autocorrelation function and elements from the same domain as the orthogonal designs. Orthogonal designs have numerous applications in Statistics, Telecommunications, Coding Theory and Cryptography, see [2, 6, 7]. An OD of order  $n$  and type  $(t_1, t_2, \dots, t_\ell)$  denoted  $OD(n; t_1, t_2, \dots, t_\ell)$  in the commuting variables  $a_1, a_2, \dots, a_\ell$ , is a square matrix  $D$  of order  $n$  with entries from the set  $\{0, \pm a_1, \pm a_2, \dots, \pm a_\ell\}$  satisfying  $DD^T = \sum_{i=1}^{\ell} (t_i a_i^2) I_n$ , where  $I_n$  is the identity matrix of order  $n$ .

Our approach is twofold; firstly we develop an algebraic framework that models properties of complementary sequences. In this manner, we can apply tools from symbolic computation, i.e., Gröbner bases, to algorithmically treat complementary sequences. Our goal is to obtain an effective (algorithmic) version of the reverse of the celebrated Equating/Killing Lemma in the theory of orthogonal designs.

**Lemma 1** (Equating and Killing Lemma [2]). *If  $D$  is an orthogonal design  $OD(n; t_1, t_2, \dots, t_\ell)$  in the commuting variables  $\{0, \pm a_1, \pm a_2, \dots, \pm a_\ell\}$ , then there exist orthogonal designs:*

$$(i) \quad OD(n; t_1, t_2, \dots, t_i + t_j, \dots, t_\ell) \quad (a_i = a_j) \quad (\text{Equating})$$

$$(ii) \quad OD(n; t_1, t_2, \dots, t_{j-1}, t_{j+1}, \dots, t_\ell) \quad (a_j = 0) \quad (\text{Killing})$$

on the  $u - 1$  commuting variables  $\{0, \pm a_1, \pm a_2, \dots, \pm a_{j-1}, \pm a_{j+1}, \dots, \pm a_\ell\}$ .

Sequences of zero autocorrelation give rise to ODs, for more details see [2, 6, 7]. In this work, we focus on the level of complementary sequences instead of ODs. In particular, given a set of complementary sequences of type  $(t_1, t_2, \dots, t_\ell)$ , we investigate how to compute a new set of complementary sequences of type  $(t_1, t_2, \dots, t_{i-1}, a, b, t_{i+1}, \dots, t_\ell)$  and another set of complementary sequences of type  $(t_1, t_2, \dots, t_\ell, t_{\ell+1})$  (if possible, otherwise decide it is impossible). In the aftermath, these sets of sequences can be used in suitable arrays to generate the desired ODs.

\*This work was carried out during the tenure of an ERCIM “Alain Bensoussan” Fellowship Programme. This Programme is supported by the Marie Curie Co-funding of Regional, National and International Programmes (COFUND) of the European Commission. In addition, this work was funded by COMET K1, FFG - Austrian Research Promotion Agency.

†This research was partially supported by Austrian Science Fund (FWF) grants P20347-N18 and P22748-N18.

## 2 Complementary Sequences

### 2.1 Notation

Let  $A = \{a_1, a_2, \dots, a_\ell\}$  be a set of  $\ell$  variables. We denote by  $\mathcal{S}^{A,n}$  the set of sequences of length  $n$  containing elements from  $\{\pm a_1, \pm a_2, \dots, \pm a_\ell\} \cup \{0\}$ . Given  $k$  sequences  $S_i \in \mathcal{S}^{A,n}$  for  $i \in [k]$ , we define the  $k$ -tuple  $T$  to be the sequence  $T = (S_i)_{i \in [k]}$ , where  $[k] = \{1, \dots, k\}$ . The set of all  $k$ -tuples containing sequences from  $\mathcal{S}^{A,n}$  is denoted by  $\mathbb{T}_k^{n,\ell}$ . We note that the names of the variables are not essential, thus for denoting  $\mathbb{T}_k^{n,\ell}$ ,  $\ell$  is sufficient and  $A$  is not needed.

Given a sequence  $S$  we denote by  $[S]_a$  the number of occurrences of  $\pm a$  in  $S$ . We extend the definition for tuples in a natural way, as follows. For  $T \in \mathbb{T}_k^{n,\ell}$ , we have

$$[T]_i = \sum_{j=1}^k [S_j]_i.$$

**Definition 2** (Type). *Given a tuple  $T \in \mathbb{T}_k^{n,\ell}$  with elements from  $\{a_1, a_2, \dots, a_\ell\}$ , we define its type, denoted  $\mathcal{T}(T)$ , to be  $(t_1, t_2, \dots, t_\ell)$  if  $t_i = [T]_{a_i}$  for  $i \in [\ell]$ .*

### 2.2 Autocorrelation Function

Let  $T \in \mathbb{T}_k^{n,\ell}$ , then we define the *non-periodic autocorrelation function*  $\text{NPAF}_T(s)$  (abbreviated as  $\text{NPAF}$ ) of  $T$  as

$$\text{NPAF}_T(s) = \sum_{j=1}^k \sum_{i=1}^{n-s} S_{j_i} S_{j_{i+s}} \quad (1)$$

for  $s = 0, 1, \dots, n-1$  and the *periodic autocorrelation function*  $\text{PAF}_T(s)$  (abbreviated as  $\text{PAF}$ ) of  $T$ , is defined, reducing  $i+s$  modulo  $n$ , as

$$\text{PAF}_T(s) = \sum_{j=1}^k \sum_{i=1}^n S_{j_i} S_{j_{i+s}} \quad (2)$$

for  $s = 0, 1, \dots, n-1$ .

It is clear that  $\text{PAF}_T(s) = \text{NPAF}_T(s) + \text{NPAF}_T(n-s)$ , for  $s = 1, \dots, n-1$ . Therefore, if  $\text{NPAF}_T(s) = 0$  for all  $s = 1, \dots, n-1$ , then  $\text{PAF}_T(s) = 0$  for all  $s = 1, \dots, n-1$ . But,  $\text{PAF}_T(s)$  may equal zero for all  $s = 1, \dots, n-1$ , even if the  $\text{NPAF}_T(s)$  are not.

**Definition 3.** *Let  $T \in \mathbb{T}_k^{n,\ell}$  with  $\mathcal{T}(T) = (t_1, t_2, \dots, t_\ell)$ . We say that  $T$  is  $k$ - $\text{PAF}(n; t_1, t_2, \dots, t_\ell)$  (resp.  $k$ - $\text{NPAF}(n; t_1, t_2, \dots, t_\ell)$ ) if  $T$  has zero  $\text{PAF}$  (resp.  $\text{NPAF}$ ), i.e.,  $\text{PAF}_T(s) = 0$  (resp.  $\text{NPAF}_T(s) = 0$ ) for  $s = 1, \dots, n-1$ .*

**Remark 4.** Recall that the  $k$ -tuple  $T \in \mathbb{T}_k^{n,\ell}$  was defined as a tuple of sequences  $S_i \in \mathcal{S}^{A,n}$  for  $i \in [k]$ . When the assumptions of definition 3 hold, we say that the  $k$ -tuple  $T$  is a tuple of complementary sequences.

For more details on complementary sequences and their application in the construction of ODs we refer the interested reader to [2, 3, 4, 7].

In order to unify notation and since the distinction is not essential for the rest of the model, we will use  $\text{AF}_T$  to denote the autocorrelation function ( $\text{AF}$ ) of a tuple  $T$ , irrelevant of whether it is the non-periodic or the periodic one. When needed, the distinction will be made clear by context.

Let  $T \in \mathbb{T}_k^{n,\ell}$ , then

$$\text{AF}_T(s) = \sum_{j=1}^k \sum_{i=1}^p S_{j_i} S_{j_{i+s}} \quad (3)$$

for  $s = 0, 1, \dots, n-1$ . As already mentioned we are interested only in the two possible types of  $\text{AF}$  defined previously, namely the non-periodic  $\text{AF}$  where  $p = n-s$  (c.f. Eq. 1) and the periodic  $\text{AF}$  where  $p = n$  and  $i+s$  is computed modulo  $n$  (c.f. Eq. 2).

Finally, we would like to mention that this work is an extension of our previous approach to provide an algebraic framework for complementary sequences [5].



### 3 An Algebraic Model for Complementary Sequences

The goal of this section is to develop an algebraic framework for the manipulation of complementary sequences. The three problems we consider are SPLIT, FILL and EXPAND, where SPLIT is the reverse of Equating while FILL and EXPAND are the reverse of Killing. Given a tuple  $T \in \mathbb{T}_k^{n,\ell}$  with  $\mathcal{T} = (t_1, t_2, \dots, t_\ell)$ , we will construct three algebraic systems  $S_s, S_f$  and  $S_e$  whose solutions give rise to tuples in  $\mathbb{T}_k^{n,\ell}$  with types:

SPLIT	FILL	EXPAND
$(t_1, \dots, t_{i-1}, \mathbf{t}, t_i - \mathbf{t}, t_{i+1}, \dots, t_\ell)$ for some $\mathbf{t} \in [t_i - 1]$	$(t_1, t_2, \dots, t_i, \mathbf{t}, t_{i+1}, \dots, t_\ell)$ for some $\mathbf{t} \in [kn - \sum_{i=1}^{\ell} t_i]$	$(t_1, t_2, \dots, t_i + \mathbf{t}, \dots, t_\ell)$ for some $\mathbf{t} \in [kn - \sum_{i=1}^{\ell} t_i]$
The first step is to introduce new variables $x_i$ and substitute accordingly in the tuple:		
SPLIT	FILL	EXPAND
$x_i$ for $i \in [t_i]$ and substitute the $j$ -th occurrence of $a_i$ by $x_j$	$x_i$ for $i \in [kn - \sum_{i=1}^{\ell} t_i]$ and substitute the $j$ -th 0 by $x_j$	$x_i$ for $i \in [kn - \sum_{i=1}^{\ell} t_i]$ and substitute the $j$ -th 0 by $x_j$

Now we have a tuple of sequences where each position that is candidate to change is assigned to a new variable. We denote by  $m$  the number of new variables (this varies depending on the problem). We denote this tuple by  $T'$  and note that this tuple no longer belongs to  $\mathbb{T}_k^{n,\ell}$ , but in  $\mathbb{T}_k^{n,\ell+m}$ . In order to construct an algebraic model we need to express autocorrelation relations and the type of a tuple algebraically. Moreover, the variables should be bounded and discrete. Although structurally the algebraic systems are the same for all three problems, at each step, the polynomials added in the system are slightly different. Let  $\mathcal{R} = \mathbb{Q}[a_1, a_2, \dots, a_\ell, x_1, x_2, \dots, x_m]$  be the polynomial ring in  $\ell + m$  variables over the field of rational numbers.

**Zero autocorrelation** In order to encode autocorrelation algebraically, we observe that the expression for the autocorrelation function is already a polynomial one. It is clear that  $\text{AF}_{T'}(s) \in \mathcal{R}$  for  $s = 0, 1, \dots, n - 1$ , i.e.,  $\text{AF}_{T'}(s)$  is a polynomial in the variables  $a_1, a_2, \dots, a_\ell, x_1, x_2, \dots, x_m$ . The algebraic conditions for the new tuple, where in the position of  $x_i$  we put the value indicated by the root of the system, being a  $k$ -AF tuple is that these polynomials are zero.

**Bounded Discrete Variables** By bounded discrete variable, we mean a variable that takes values from a finite subset of the integers. We need to restrict the solutions of the algebraic systems to take particular values in order to use the solutions to construct new tuples with the desired types. It is easy to see that for  $f_i \in \mathbb{K}[x_1, x_2, \dots, x_m]$  we have  $V(\langle f_1, f_2, \dots, f_k \rangle) \cap M^m = V(\langle f_1, f_2, \dots, f_k, b_1, b_2, \dots, b_m \rangle)$ , where  $b_i = \prod_{\alpha \in M} (x_i - \alpha)$  and  $M$  is a finite subset of the algebraic closure of  $\mathbb{K}$ .

It is exactly these polynomials  $b_i$  that we need to add to the respective algebraic systems for each of the problems, depending on what set we want the solutions to be restricted in.

SPLIT	FILL	EXPAND
$b_i = x_i^4 - 1$ $x_i \in \{\pm 1, \pm i\}$	$b_i = x_i(x_i^2 - 1)$ $x_i \in \{0, \pm 1\}$	$b_i = x_i(x_i^2 - a^2)$ $x_i \in \{0, \pm a\}$

The choice for these values is justified since for SPLIT we want to introduce two new (signed) symbols in the tuple, for FILL we want to introduce one new (signed) symbol but we should allow for zeros to remain zeros and for EXPAND we want to introduce no new symbol, but use the existing one that is being expanded and allow for possible zeros.

**Type Conditions** We need conditions that force a certain type for the new tuple. For this we use two polynomials, one relating the  $x_i$  variables to the variable  $x_t$  and one that forces  $x_t$  to take discrete values in a feasible range  $\{1, 2, \dots, B\}$ .

For SPLIT we have that a variable  $a$  can be split into two variables of type  $x_t$  and  $[T]_a - x_t$  for  $1 \leq x_t \leq \lfloor \frac{[T]_a}{2} \rfloor$ . For FILL and EXPAND we have that a variable (new or existing respectively) can replace up to  $kn - \sum_{i=1}^{\ell} t_i$  zeros. Thus the type conditions consist of two polynomials as follows:

SPLIT	FILL	EXPAND
$B = \lfloor \frac{[T]_a}{2} \rfloor$ $T_1 = \prod_{i=1}^B (x_t - i)$ $T_2 = (\sum_{i=1}^m x_i^2) - m + 2x_t$	$B = kn - \sum_{i=1}^{\ell} t_i$ $T_1 = \prod_{i=1}^B (x_t - i)$ $T_2 = (\sum_{i=1}^m x_i^2) - x_t$	$B = kn - \sum_{i=1}^{\ell} t_i$ $T_1 = \prod_{i=1}^B (x_t - i)$ $T_2 = (\sum_{i=1}^m x_i^2) - a^2([T']_a + x_t)$

**The algebraic system** According to the discussion above, we have that the three algebraic systems  $S_s, S_f$  and  $S_e$  are as follows:

SPLIT	FILL	EXPAND
$S_s = \left\{ \begin{array}{l} \text{AF}_{T'}(s) \text{ for } s \in [n] \\ B_i = x_i^4 - 1, i \in [m] \\ T_1 = \prod_{i=1}^B (x_t - i) \\ T_2 = \left( \sum_{i=1}^m x_i^2 \right) - m + 2x_t \end{array} \right\}$	$S_f = \left\{ \begin{array}{l} \text{AF}_{T'}(s) \text{ for } s \in [n] \\ B_i = x_i (x_i^2 - 1), i \in [m] \\ T_1 = \prod_{i=1}^B (x_t - i) \\ T_2 = \left( \sum_{i=1}^m x_i^2 \right) - x_t \end{array} \right\}$	$S_e = \left\{ \begin{array}{l} \text{AF}_{T'}(s), s \in [n] \\ B_i = x_i (x_i^2 - a^2), i \in [m] \\ T_1 = \prod_{i=1}^B (x_t - i) \\ T_2 = \left( \sum_{i=1}^m x_i^2 \right) - a^2 \left( [T']_a + x_t \right) \end{array} \right\}$

**Retrieving the solutions** The algebraic systems  $S_s, S_f$  and  $S_e$  provide us with solutions to the three problems at hand. The last step we need to take is to interpret a root of the system and connect it to a new tuple of complementary sequences. Assume that  $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_m)$  is such a root of the respective algebraic system. Then we create a new tuple making substitutions in  $T'$  as follows:

SPLIT	FILL	EXPAND
$\left\{ \begin{array}{l} \text{if } \alpha_i = 1 \text{ then } x_i = a \\ \text{if } \alpha_i = -1 \text{ then } x_i = -a \\ \text{if } \alpha_i = i \text{ then } x_i = b \\ \text{if } \alpha_i = -i \text{ then } x_i = b \end{array} \right\}$	$\left\{ \begin{array}{l} \text{if } \alpha_i = 0 \text{ then } x_i = 0 \\ \text{if } \alpha_i = 1 \text{ then } x_i = a \\ \text{if } \alpha_i = -1 \text{ then } x_i = -a \end{array} \right\}$	$\left\{ \begin{array}{l} \text{if } \alpha_i = 0 \text{ then } x_i = 0 \\ \text{if } \alpha_i = a \text{ then } x_i = a \\ \text{if } \alpha_i = -a \text{ then } x_i = -a \end{array} \right\}$

We note that since the solution set is zero dimensional (finite number of possible values for a finite number of variables). This means that the reduced Gröbner Basis for a lexicographic (elimination) order will have a triangular form [1].

It is important to mention that the variables  $a_i$  appear in the algebraic system we constructed. Nevertheless, due to the independence of the solutions with respect to the variables  $x_i$  from the variables  $a_i$ , we can project by choosing random values for the variables  $a_i$ . There is a finite set of evaluations of the variables  $a_i$  that affects the projected variety of the algebraic system. Since we treat the variables  $a_i$  as parameters, we are not interested in these evaluations. In other words, by substituting the variables  $a_i$  by random values from an infinite set, the part of the solutions of the system that corresponds to the variables  $x_i$  remains unchanged with probability 1.

**Examples** Given a tuple  $T$  we apply the algorithm described above to construct an algebraic system, find a solution to the system and interpret accordingly to construct a new tuple of the desired type:

SPLIT	EXPAND
$T = (a, b, a) (a, b, -a) (b, -a, b) (b, d, -b)$ $\mathcal{T}((a, b, a) (a, b, -a) (b, -a, b) (b, d, -b)) = (1, 5, 6)$ $T' = (x_1, b, x_2) (x_3, b, x_4) (b, x_5, b) (b, d, -b)$ $\left\{ \begin{array}{l} b * x_1 + b * x_2 + b * x_3 + b * x_4 + 2 * b * x_5, \\ x_1 * x_2 + x_3 * x_4, \\ x_1^4 - 1, x_2^4 - 1, \\ x_3^4 - 1, x_4^4 - 1, \\ x_5^4 - 1, \\ x_t^2 - 3 * x_t + 2, \\ x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 + 2 * x_t - 5 \end{array} \right\}$ <p>Solution: <math>\alpha = (i, -1, -1, -i, 1)</math> and <math>x_t = 2</math></p> <p>Substitution: <math>(x_1, x_2, x_3, x_4, x_5) = (a, -c, -c, -a, c)</math></p> <p>New tuple: <math>(a, b, -c) (-c, b, -a) (b, c, b) (b, d, -b)</math></p> $\mathcal{T}((a, b, -c) (-c, b, -a) (b, c, b) (b, d, -b)) = (1, 2, 3, 6)$	$T = (0, b, 0) (0, b, 0) (b, 0, b) (b, d, -b)$ $\mathcal{T}((0, b, 0) (0, b, 0) (b, 0, b) (b, d, -b)) = (1, 6)$ $T' = (x_1, b, x_2) (x_3, b, x_4) (b, x_5, b) (b, d, -b)$ $b * x_1 + b * x_2 + b * x_3 + b * x_4 + 2 * b * x_5,$ $\left\{ \begin{array}{l} x_1 * x_2 + x_3 * x_4, \\ (x_1 - d)(x_1 + d)x_1, (x_2 - d)(x_2 + d)x_2, \\ (x_3 - d)(x_3 + d)x_3, (x_4 - d)(x_4 + d)x_4, \\ (x_5 - d)(x_5 + d)x_5, d^2 - 1, \\ x_t^5 - 15 * x_t^4 + 85 * x_t^3 - 225 * x_t^2 + 274 * x_t - 120, \\ x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 - x_t \end{array} \right\}$ <p>Solution: <math>\alpha = (1, 1, 1, -1, -1)</math> and <math>x_t = 5</math></p> <p>Substitution: <math>(x_1, x_2, x_3, x_4, x_5) = (d, d, d, -d, -d)</math></p> <p>New tuple: <math>(d, b, d) (d, b, -d) (b, -d, b) (b, d, -b)</math></p> $\mathcal{T}((d, b, d) (d, b, -d) (b, -d, b) (b, d, -b)) = (6, 6)$

## 4 Conclusion

In this paper, we dealt with the problem of constructing new tuples of complementary sequences from a given tuple of complementary sequences on  $\ell$  variables, providing an algorithmic version of the reverse of the Equating-Killing Lemma.

We describe the construction of three algebraic systems, solving the three problems that reverse the Equating-Killing Lemma, namely SPLIT, FILL, EXPAND. This construction is algorithmic and thus, if combined with the use of Gröbner bases, it provides a fully algorithmic framework for the computation of new tuples of complementary sequences.

We employ Gröbner bases, in order to get a convenient description of the ideal of the (zero dimensional) variety we are interested in. The variety provides full information concerning the possible ways to SPLIT a variable, FILL the zeros or EXPAND a variable in a given  $k$ -tuple  $T$  of complementary sequences.

Our goal is to provide an algebraic model for complementary sequences which can be used to generate orthogonal designs. Conditioned that the algorithmic implementations of the proposed framework retrieve the desired properties for complementary sequences, our next step is to model the statistical properties of orthogonal designs (orthogonality, interactions) again in terms of complementary sequences. This statistical modelling of complementary sequences together with the algorithmic implementations of SPLIT, FILL, EXPAND, will be further explored in future work.

## References

- [1] D. Cox, J. Little, and D. O’Shea. *Ideals, Varieties, and Algorithms : An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992.
- [2] A. V. Geramita and J. Seberry. *Orthogonal designs. Quadratic forms and Hadamard matrices*, volume 45 of *Lecture Notes in Pure and Applied Mathematics*. Marcel Dekker, Inc., New York, NY, 1979.
- [3] C. Koukouvinos. Sequences with zero autocorrelation. In C. J. Colbourn and J. H. Dinitz, editors, *The CRC Handbook of Combinatorial Designs*, pages 452–456. CRC Press, Boca Raton, Fla., 1996.
- [4] C. Koukouvinos and J. Seberry. New weighing matrices and orthogonal designs constructed using two sequences with zero autocorrelation function - a review. *J. Statist. Plann. Inference*, 81:153–182, 1999.
- [5] C. Koukouvinos, D. E. Simos, and Z. Zafeirakopoulos. An algebraic framework for extending orthogonal designs. In *ISSAC ’11: Abstracts of Poster Presentations of the 36th International Symposium on Symbolic and Algebraic Computation, ACM Commun. Comput. Algebra*, volume 45, pages 123–124, 2011.
- [6] J. Seberry and R. Craigen. Orthogonal designs. In C. J. Colbourn and J. H. Dinitz, editors, *The CRC Handbook of Combinatorial Designs*, pages 400–406. CRC Press, Boca Raton, Fla., 1996.
- [7] J. Seberry and M. Yamada. Hadamard matrices, sequences and block designs. In J. H. Dinitz and D. R. Stinson, editors, *Contemporary Design Theory: A Collection of Surveys*, pages 431–560. J. Wiley and Sons, New York, 1992.

# Goodness-of-fit testing in Ising Models

Abraham Martín del Campo, Caroline Uhler  
IST Austria

`abraham.mc@ist.ac.at`

## Abstract

Markov bases have been developed in algebraic statistics for exact goodness-of-fit testing. They connect all elements in a fiber (given by the sufficient statistics) and allow building a Markov chain to approximate the distribution of a test statistic by its posterior distribution. However, finding a Markov basis is often computationally intractable. In addition, the number of Markov steps required for converging to the stationary distribution depends on the connectivity of the sampling space.

We study the combinatorial structure of the finite lattice Ising model and propose a new method for exact goodness of fit testing which avoids computing a Markov basis. Instead, we build a Markov chain that only uses simple moves (i.e. swaps of two interior sites). These simple moves are not sufficient to create a connected Markov chain. However, by allowing a bounded change in the sufficient statistics, we prove that the resulting Markov chain is indeed connected, reversible, and aperiodic. The proposed algorithm not only overcomes the computational burden of finding a Markov basis, it might also lead to a better connectivity of the sampling space and hence a faster convergence.

## Keywords

Ising model, Monte Carlo methods, Markov chains

# Monomial ideal methods for hierarchical statistical models

Hugo Maruri-Aguillar  
Queen Mary University of London (UK)

Eduardo Sáenz de Cabezón  
Universidad de La Rioja (Spain)

Henry P Wynn  
London School of Economics (UK)

`h.maruri-aguilar@qmul.ac.uk`

## Abstract

A hierarchical statistical model can be associated with a simplicial complex  $\mathcal{S}$  in the following way. To every vertex  $i$  of  $\mathcal{S}$  we associate an input, or independent variable:  $x = (x_1, \dots, x_n)$ . To a simplex  $J$  of  $\mathcal{S}$  we associate a function of the variables  $x_J = \{x_i, i \in J\}$ , which we write  $h_J(x_J)$ . There are two types of model which are naturally associated with this set-up. The first is a model for the mean of a dependent random variable  $Y$  of the form  $\mu = \sum_{J \in \mathcal{S}} h_J(x_J)$ . For example, if  $n = 3$  and the cliques are  $\{1, 2\}$  and  $\{2, 3\}$  we have the model  $\mu_Y = h_0 + h_1(x_1) + h_2(x_2) + h_{1,2}(x_1, x_2) + h_{2,3}(x_2, x_3)$ . In the second case we have an exponential model for a multinomial probability, or distribution, attached to a support:  $p(x) = \exp(\sum_{J \in \mathcal{S}} h_J(x_J))$ . If we introduce parameters  $\theta_J$  then we write for the model part  $\sum_{J \in \mathcal{S}} \theta_J h_J(x_J)$ . Then, in the first case we have a linear regression model for the mean of the random and in the second case a log-linear model with a natural exponential family representation [1].

We are interested, in both cases, in the relationship between the structure of the model as given by  $\mathcal{S}$  and the Stanley Reisner ideal  $I_{\mathcal{S}}$  of  $\mathcal{S}$ . This is generated by all square-free monomials corresponding to terms *not* in the model. In the above example this is just  $\langle x_1 x_3 \rangle$ , because  $\{1, 3\} \notin \mathcal{S}$ . In the regression case  $I_{\mathcal{S}}$  gives important information about the interactions and so-called *alias* structure of the model, with strong links to the theory of experimental design [2]. In the probability model case  $I_{\mathcal{S}}$  can be used to capture the conditional independent structure. An important example is when  $\mathcal{S}$  is the flag complex of a decomposable models and the Dirac theorem describes  $I_{\mathcal{S}}$ , rather precisely [3]. In general, several important features of the ideal  $I_{\mathcal{S}}$ , such as Krull dimension, Betti numbers, Hilbert series and Alexander duality, have implications for the modelling.

By considering different functions (kernels)  $h_J(x_J)$  we can cover hierarchical modeling for a wide range of situations.

## Keywords

monomial ideals, hierarchical models, algebraic statistics

## References

- [1] M. Drton, B. Sturmfels, and S. Sullivant, *Lectures on Algebraic Statistics*. Birkhauser, 2009.
- [2] H. Maruri-Aguilar, E. S. de Cabezón, and H. P. Wynn, “Betti numbers of polynomial hierarchical models for experimental designs,” *Ann. Math. Artif. Intell.*, vol. 64, no. 4, pp. 411–426, 2012.
- [3] J. Herzog and T. Hibi, *Monomial ideals*. Springer, 2011.

# Algebraic geometry in causal inference

Caroline Uhler  
IST, Austria

`caroline.uhler@ist.ac.at`

## Abstract

Many algorithms for inferring causality are based on partial correlation testing and rely heavily on the strong-faithfulness assumption. In the Gaussian setting, the set of strong-unfaithful distributions corresponds to a collection of fattened-up hypersurfaces, which are defined by partial correlations. Interestingly, as we explain in this talk, the volume of the strong-unfaithful distributions depends on the complexity of the singularities (measured by their real log canonical threshold) of the defining hypersurfaces. Studying these hypersurfaces, we show that the strong-faithfulness assumption is extremely restrictive, implying fundamental limitations for causal inference algorithms based on partial correlations, with the PC-algorithm as its most prominent example.

In the second part of the talk, we propose an alternative algorithm, which is based on finding the permutation of the variables that yields the sparsest directed acyclic graph. In the Gaussian setting, this algorithm boils down to finding the sparsest Cholesky decomposition of a matrix. We prove that the constraints required for our algorithm are strictly weaker than strong-faithfulness and are necessary for any causal inference algorithm based on partial correlation testing.

## Keywords

Causal inference, directed Gaussian graphical model, partial correlation testing, algebraic hypersurface, real singularity, sparse Cholesky decomposition

# Connectivity on two-way tables under certain models

Ruriko Yoshida  
University of Kentucky

ruriko.yoshida@uky.edu

## Abstract

We first consider the two-way contingency tables under several different models, namely, the diagonal model, the independence model with cell upper bounds and with structural zeros, and the quasi-independence model. Then we showed that if we allow each cell to be  $-1$ , then  $2 \times 2$  minor basic moves connect all tables in a fiber under each model. In the end we proposed an algorithm to connect all tables in a fiber under a given model by moves in a subset of a *Markov basis* for the model by allowing each cell to be  $-1$  in a general set up.

## Keywords

Basic moves, contingency tables, Markov bases

We consider two-way tables under various models. Let  $r, c \geq 2$  and  $r, c \in \mathbb{Z}$ . Let  $\mathcal{I}$  be an index set, i.e.

$$\mathcal{I} = \{(i, j) : 1 \leq i \leq r, 1 \leq j \leq c\}.$$

Here we consider a two way  $r \times c$  contingency table  $\mathbf{X} = (n_{ij})_{(i,j) \in \mathcal{I}}$  and we consider the several models such as

- Diagonal models
- Independence model with cell upper bounds
- The structural zero problem
- The quasi-independence model.

We first define a “basic move”.

**Definition 1** Let  $b$  be a  $r \times c$  table such that

	$j$	$j'$
$i$	1	$-1$
$i'$	$-1$	1

where  $1 \leq i, i' \leq r$ ,  $1 \leq j, j' \leq c$ ,  $i \neq i'$ ,  $j \neq j'$  and other cells are all zero. We call  $\pm b$  a basic move. We denote this table  $b$  as  $(i, i'; j, j')$ .

Let  $M$  be a set of all basic moves.

First consider the *independence model*. Let  $\{X_{ij}\}$  be a table of counts whose entries are independent geometric random variables with canonical parameters,  $\{\theta_{ij}\}$ . Consider the generalized linear model,

$$\theta_{ij} = \lambda + \lambda_i^R + \lambda_j^C \tag{1}$$

for  $i = 1, \dots, r$  and  $j = 1, \dots, c$ , where  $R$  and  $C$  denote the nominal-scale row and column factors. Notice that the row and column margins are sufficient statistics for this model. Hence, the conditional distribution of the table counts given the margins is the same regardless of the values of the parameters in the model. We consider  $\mathbf{b}_{ind}$  as a column vector with dimension  $r + c$ . We also order the elements of  $X$  with respect to a lexicographic order and regard  $X$  as a column vector with dimension  $|\mathcal{I}|$ . Then the relation between  $X$  and  $\mathbf{b}_{ind}$  is written by

$$A_{ind}X = \mathbf{b}_{ind}, \tag{2}$$

which represents the system of equations for the row and column sums. Here  $A_{ind}$  is an  $(r+c) \times |\mathcal{I}|$  matrix consisting of 0's and 1's. In general such matrix which defines the system of equalities for the sufficient statistics is called *design matrix*. The set of tables  $X \in \mathbb{N}^{\mathcal{I}}$  satisfying (2) is called the *fiber* for  $\mathbf{b}_{ind}$  and is denoted by  $\mathcal{F}_{ind}(\mathbf{b}_{ind})$  such that

$$\mathcal{F}_{ind}(\mathbf{b}_{ind}) = \{X \in \mathbb{N}^{\mathcal{I}} | A_{ind}X = \mathbf{b}_{ind}\}.$$

The following theorem is fairly well-known:

**Theorem 2** ([5]) *All moves in  $M$  connect all two-way contingency tables under the independence model  $\mathcal{F}_{ind}(\mathbf{b}_{ind})$  for any  $\mathbf{b}_{ind}$  with  $\mathcal{F}_{ind}(\mathbf{b}_{ind}) \neq \emptyset$ .*

The idea of allowing some entries to drop down to  $-1$  appears in [1] and [3]. In high-dimensional tables ( $r+c$  large), the enlarged state space that allows entries to drop down to  $-1$  may be much larger than the set of interest  $F_{\mathbf{n}}$ , even though each dimension is only slightly extended. Nevertheless, in this paper, we consider several different models for two-way contingency table and we show the connectivity of the tables under each model by moves in  $M$  by allowing some entries to drop down to  $-1$ .

## 1 Models

In this section we define models we consider. Now, let  $\{X_{ij}\}$  be a table of counts whose entries are independent geometric random variables with canonical parameters,  $\{\theta_{ij}\}$ . The most general loglinear association model for an  $r \times c$  contingency table has a canonical linear predictor of the form

$$\theta_{ij} = \lambda + \lambda_i^R + \lambda_j^C + \lambda_{ij}^{RC} \quad (3)$$

for  $i = 1, \dots, r$  and  $j = 1, \dots, c$ .

### 1.1 Diagonal model

The diagonal model is a model with extra constraints to the Independence model such that  $\lambda_{ij}^{RC} = 0$  if  $i \neq j$  and  $\lambda_{ii}^{RC} = \lambda$ , association models. Under this model, the sufficient statistic consists of the row sums, column sums and the sum of the diagonal frequencies:

$$x_{i+} = \sum_{j=1}^c x_{ij}, \quad i = 1, \dots, r, \quad x_{+j} = \sum_{i=1}^r x_{ij}, \quad j = 1, \dots, c, \quad x_D = \sum_{i=1}^{\min(r,c)} x_{ii}.$$

We write the sufficient statistic as a column vector

$$\mathbf{b}_D = (x_{1+}, \dots, x_{r+}, x_{+1}, \dots, x_{+c}, x_D)'$$

We also order the elements of  $\mathbf{x}$  lexicographically and regard  $\mathbf{x}$  as a column vector. Then the relation between  $X$  and  $\mathbf{b}_D$  is written by

$$A_D X = \mathbf{b}_D, \quad (4)$$

which represents the system of equations for the row and column sums, and the diagonal sum. Here  $A_D$  is an  $(r+c+1) \times |\mathcal{I}|$  matrix consisting of 0's and 1's. The set of tables  $X \in \mathbb{N}^{\mathcal{I}}$  satisfying (4) is denoted by  $\mathcal{F}_D(\mathbf{b}_D)$  such that

$$\mathcal{F}_D(\mathbf{b}_D) = \{X \in \mathbb{N}^{\mathcal{I}} | A_D X = \mathbf{b}_D\}.$$

### 1.2 Independence model with cell upper bounds

This is a model with extra constraints to the Independence model such that each cell count  $X_{ij}$  for  $(i, j) \in \mathcal{I}$  has an upper bound. Thus we have the system of equations

$$A_{ind}X = \mathbf{b}_{ind}, \quad 0 \leq X_{i,j} \leq U_{(i,j)}, \quad (i, j) \in \mathcal{I} \quad (5)$$

which represents the system of equations for the row and column sums, and constraints for the upper bounds  $U_{(i,j)}$ . The set of tables  $X \in \mathbb{N}^{\mathcal{I}}$  satisfying (5) is denoted by  $\mathcal{F}_{bdd}(\mathbf{b}_{ind})$  such that

$$\mathcal{F}_{bdd}(\mathbf{b}_{ind}) = \{X \in \mathbb{N}^{\mathcal{I}} | A_{ind}X = \mathbf{b}_{ind}, \quad 0 \leq X_{i,j} \leq U_{(i,j)}, \quad (i, j) \in \mathcal{I}\}.$$



### 1.3 Structural zero problem

Consider the independence model for two way contingency tables. Structural zeros are a subset  $S$  of  $\mathcal{I}$  such that the probability to see an observation for  $(i, j) \in S$  is equal to zero. In fact this is a special case of the independence model with upper bounds such that  $U_{(i,j)} = 0$  for  $(i, j) \in S$ .

### 1.4 Quasi-independence model

In the quasi-independence model, the cell probabilities  $\{p_{ij}\}$  are modeled as

$$\log p_{ij} = \lambda + \lambda_i^R + \lambda_j^C + \gamma_i \delta_{ij}, \quad (6)$$

where  $\delta_{ij}$  is Kronecker's delta. In (6) each diagonal cell  $(i, i)$ ,  $i = 1, \dots, \min(r, c)$ , has its own free parameter  $\gamma_i$ . This implies that in the maximum likelihood estimation each diagonal cell is perfectly fitted:

$$\hat{p}_{ii} = \frac{x_{ii}}{n},$$

where  $n = \sum_{i=1}^R \sum_{j=1}^C x_{ij}$  is the total frequency. Since diagonal elements in each sampled table are fixed, we proceed the following process in order to sample a table under the quasi-independence model: (1) Suppose  $x = (x_{11}, x_{12}, \dots, x_{rc})$  is the observed table. Suppose (WLOG)  $r \leq c$ . We set a column vector

$$\mathbf{b}_Q = (x_{1+} - x_{11}, \dots, x_{r+} - x_{rr}, x_{+1} - x_{11}, \dots, x_{+r} - x_{rr}, x_{+(r+1)}, \dots, x_{+c})'.$$

Then the relation between  $X$  and  $\mathbf{b}_Q$  is written by

$$A_Q X = \mathbf{b}_Q, \quad (7)$$

which represents the system of equations for the row and column sums, and the diagonal sum. Here  $A_Q$  is an  $(r+c) \times |\mathcal{I}|$  matrix consisting of 0's and 1's. The set of tables  $X \in \mathbb{N}^{\mathcal{I}}$  satisfying (7) is denoted by  $\mathcal{F}_Q(\mathbf{b}_Q)$  such that

$$\mathcal{F}_Q(\mathbf{b}_Q) = \{X \in \mathbb{N}^{\mathcal{I}} | A_Q X = \mathbf{b}_Q, X_{ii} = 0, \text{ for } i = 1, \dots, r\}.$$

(2) Sample a table  $X$  from the fiber  $\mathcal{F}_Q(\mathbf{b}_Q)$ . (3) Set  $X_{ii} = x_{ii}$  for  $i = 1, \dots, r$ . Thus, this is a special case of the independence model with upper bounds such that  $U_{(i,i)} = 0$  for  $i = 1, \dots, r$ .

## 2 Markov basis and connectivity of tables

We will use the following simple observation to prove the connectivity of tables by basic moves in  $M$ .

**Remark 3** Suppose  $\mathbf{m} = \mathbf{m}_+ - \mathbf{m}_-$ , where  $\mathbf{m}_+, \mathbf{m}_- \in \mathbb{Z}_+^{|\mathcal{I}|}$ , is an element in a Markov basis for the contingency table under a certain model and if we can write

$$\mathbf{m}_+ = \mathbf{m}_- + \sum_{i=1}^k \pm b_i \text{ for some } k$$

where  $b_i \in M$  and

$$\mathbf{m}_- + \sum_{i=1}^{k_0} \pm b_i$$

has its elements greater than equal to  $-1$  for all  $0 \leq k_0 \leq k$ . If we can show this for all  $\mathbf{m}$  in a Markov basis we can show that moves in  $M$  connect to all tables in the fiber for the given model.

### 2.1 Diagonal model

In order to describe a Markov basis for the diagonal sum problem, we introduce three additional types of moves.

- Type II (indispensable moves of degree 3 for  $\min(r, c) \geq 3$ ):

$$\begin{array}{cccc} & i & i' & i'' \\ i & 0 & +1 & -1 \\ i' & -1 & 0 & +1 \\ i'' & +1 & -1 & 0 \end{array}$$

where three zeros are on the diagonal.

- Type III (dispensable moves of degree 3 for  $\min(r, c) \geq 3$ ):

$$\begin{array}{cccc} & i & i' & i'' \\ i & +1 & 0 & -1 \\ i' & 0 & -1 & +1 \\ i'' & -1 & +1 & 0 \end{array}$$

Note that given three distinct indices  $i, i', i''$ , there are three moves in the same fiber:

$$\begin{array}{ccc} +1 & 0 & -1 \\ 0 & -1 & +1 \\ -1 & +1 & 0 \end{array} \quad \begin{array}{ccc} +1 & -1 & 0 \\ -1 & 0 & +1 \\ 0 & +1 & -1 \end{array} \quad \begin{array}{ccc} 0 & -1 & +1 \\ -1 & +1 & 0 \\ +1 & 0 & -1 \end{array}$$

Any two of these suffice for the connectivity of the fiber. Therefore we can choose any two moves in this fiber for minimality of Markov basis.

- Type IV (indispensable moves of degree 4 which are non-square free):

$$\begin{array}{cccc} & j & j' & j'' \\ i & +1 & +1 & -2 \\ i' & -1 & -1 & +2 \end{array}$$

where  $i = j$  and  $i' = j'$ , i.e., two cells are on the diagonal. Note that we also include the transpose of this type as Type IV moves.

- Type V: (square free indispensable move of degree 4 for  $\max(r, c) \geq 4$ ):

$$\begin{array}{cccc} & j & j' & j'' & j''' \\ i & +1 & +1 & -1 & -1 \\ i' & -1 & -1 & +1 & +1 \end{array}$$

where  $i = j$  and  $i' = j'$ . Type V includes the transpose of this type.

Then we have the following theorem:

**Theorem 4** ([6]) *The above moves of basic moves in  $M$  and Types II-V form a Markov basis for the diagonal sum problem with  $\min(r, c) \geq 3$  and  $\max(r, c) \geq 4$ .*

By the theorem above and Remark 3 we have the following theorem:

**Theorem 5** *Consider a two way  $r \times c$  contingency table  $X_{ij}$  and we consider the diagonal model. If we allow  $X_{ij} \geq -1$ , then all moves in  $M$  connect all tables in  $\mathcal{F}_{\mathcal{D}}(\mathbf{b}_D)$ .*

## 2.2 Independence model with cell upper bounds

In 2010, Rapallo and Yoshida showed a Markov basis for this model.

**Theorem 6** (Rapallo and RY, 2010) *Moves of Type II and moves in  $M$  form a Markov basis for the independence model with cell upper bounds, i.e.,  $x_{ij} \leq U_{ij}$ ,  $(i, j) \in \mathcal{I}$ .*

Using this theorem and Remark 3 we have the following theorem

**Theorem 7** *Consider a two way  $r \times c$  contingency table  $X_{ij}$  and we consider the independence model with cell upper bounds. If we allow  $X_{ij} \geq -1$ , then all moves in  $M$  connect all tables in  $\mathcal{F}_{\text{bdd}}(\mathbf{b}_{\text{ind}})$ .*

**Remark 8** *Since the quasi-independence model and structural zero are special case of this model. This basic moves in  $M$  also connects all tables in the fiber under the quasi-independence model and structural zero.*

### 3 More general set up for arbitrary models

In this section we consider more general set up, i.e., we consider arbitrary multi-way contingency tables under an arbitrary model. In 2008, Chen, Dinwoodie, and Yoshida [2] suggested the following algorithm to connect all tables in the fiber by moves in a subset  $M$  of a Markov basis. Let  $A \in \mathbb{Z}^{n \times d}$  be a design matrix and let  $I_A$  be a *toric ideal* associate with the matrix  $A$  (see [7] for the definition of the toric ideal  $I_A$ ). Let  $\mathcal{F}_{\mathbf{b}}$  be the fiber under the model for the sufficient statistics  $\mathbf{b}$ .

When one allows entries in the table to go negative, connecting Markov chains are easier to find. The following proposition uses some standard terminology. Let  $M := \{\pm \mathbf{a}_i \in \mathbb{Z}^d : i = 1, \dots, g\} \subset \ker(A)$  be signed Markov moves (that is, integer vectors in  $\ker(A)$  that are added or subtracted randomly from the current state), not necessarily a Markov basis. Let  $I_M := \langle \mathbf{x}^{\mathbf{a}_i^+} - \mathbf{x}^{\mathbf{a}_i^-}, i = 1, \dots, g \rangle$  be the corresponding ideal, which satisfies  $I_M \subset I_A$ . The *radical* of an ideal  $I$  is  $\sqrt{I} = \{f \in Q[\mathbf{x}] : f^i \in I \text{ for some } i \in \mathbb{Z}_+\}$ . If  $I = \sqrt{I}$ , then we say that  $I$  is a *radical ideal* (p. 35 of [4]).

A set of integer vectors  $M \subset \mathbb{Z}^c$  is called a *lattice basis* for  $A$  if every integer vector in  $\ker(A)$  can be written as an integral linear combination of the vectors (or moves) in  $M$ . Computing a lattice basis is very simple and does not require symbolic computation.

**Proposition 9** ([2]) *Suppose  $I_M$  is a radical ideal, and suppose the moves in  $M$  form a lattice basis. Then the Markov chain using the moves in  $M$  that allows entries to drop down to  $-1$  connects a set that includes the set  $\mathcal{F}_{\mathbf{b}}$ .*

Proposition 9 makes it possible to use the following approach on large tables: compute a lattice basis, compute the radical of the ideal of binomials from the lattice basis, run the Markov chain in the larger state space, and do computations on  $\mathcal{F}_{\mathbf{b}}$  by conditioning. To be precise, suppose  $\mathcal{F}_{\mathbf{b}} \subset \mathcal{F}_0$  where the set  $\mathcal{F}_0$  is the connected component of the Markov chain that is allowed to drop down to  $-1$  as above. Suppose the desired sampling distribution  $\mu$  on  $\mathcal{F}_{\mathbf{b}}$  is uniform. If one runs a symmetric Markov chain  $X_1, X_2, X_3, \dots, X_n$  in  $\mathcal{F}_0$ , then a Monte Carlo estimate of  $\mu(F)$  for any subset  $F \subset \mathcal{F}_{\mathbf{b}}$  is

$$\mu(F) = \frac{\sum_{i=1}^n \mathbf{I}_F(X_i)}{\sum_{i=1}^n \mathbf{I}_{\mathcal{F}_{\mathbf{b}}}(X_i)}$$

where  $\mathbf{I}_F$  is the indicator function of the set  $A$ .

## References

- [1] F. Bunea and J. Besag. *MCMC in  $I \times J \times K$  contingency tables*, pages 25–36. American Mathematical Society, Providence, Rhode Island, 2000. in *Monte Carlo Methods*.
- [2] Y. Chen, I. Dinwoodie, and R. Yoshida. *Markov Chains, Quotient Ideals, and Connectivity with Positive Margins*, pages 99 – 110. Cambridge, 2008. in *Algebraic and Geometric Methods in Statistics* dedicated to Professor Giovanni Pistone (P. Gibilisco, E. Riccomagno, M.-P. Rogantin, H. P. Wynn, eds.).
- [3] Y. Chen, I. H. Dinwoodie, A. Dobra, and M. Huber. *Lattice points, contingency tables and sampling*, pages 65–78. American Mathematical Society, 2005. in *Integer Points in Polyhedra–Geometry, Number Theory, Algebra, Optimization*. A. Barvinok, M. Beck, C. Haase, B. Reznick and V. Welker eds.
- [4] D. Cox, J. Little, and D. O’Shea. *Ideals, Varieties, and Algorithms*. Springer, New York, NY, 2nd edition edition, 1997.
- [5] P. Diaconis and B. Sturmfels. Algebraic algorithms for sampling from conditional distributions. *Ann. Statist.*, 26(1):363–397, 1998.
- [6] H. Hara, A. Takemura, and R. Yoshida. A markov basis for conditional test of common diagonal effect in quasi-independence model for two-way contingency tables. *J of Computational Statistics and Data Analysis*, 53:1006 – 1014, 2009.
- [7] Bernd Sturmfels. *Gröbner Bases and Convex Polytopes*, volume 8 of *University Lecture Series*. American Mathematical Society, Providence, RI, 1996.



---

---

# Session 9: Computer algebra, quantum computing and quantum information processing

---

---

Organizers:

Vladimir Gerdt  
Alexander Prokopenya  
Yoshia Uwano



# On the inequalities defining the entanglement space of 2-qubits

V.P.Gerdt <sup>a</sup>, A.M.Khvedelidze <sup>a,b,c</sup> and Yu.G.Palii <sup>b</sup>  
<sup>a</sup> Joint Institute for Nuclear Research, Dubna, Russia  
<sup>b</sup> A Razmadze Mathematical Institute, Tbilisi, Georgia  
<sup>c</sup> University of Georgia, Tbilisi, Georgia

gerdt@jinr.ru

## Abstract

The issue of description of the *entanglement space*  $\mathcal{E}_2$ , i.e., the orbit space  $\mathfrak{P}_+/G$ , where  $\mathfrak{P}_+$  - the space of mixed states of pair of qubits,  $G = U(2) \otimes U(2)$  - the group of so-called local unitary transformations, is discussed. Within the geometrical invariant theory, using the integrity basis for the ring of  $G$ -invariant polynomials, the derivation of equations and inequalities that determine the entanglement space  $\mathcal{E}_2$  are outlined.

## Keywords

Quantum computation, density matrix, entanglement, orbit space, local invariants, polynomial inequalities

## 1 Quantum non-localities and orbit space

A motivation to study the orbits space  $\mathfrak{P}_+/G$  for  $d$ -dimensional  $r$ -partite quantum system is as follows. A state  $\varrho \in \mathfrak{P}_+$ , characterizing a composite quantum system is an element of the tensor product of Hilbert-Schmidt spaces of operators corresponding to each  $r$  individual subsystem. In accordance with a fixed factorization  $d = n_1 \times n_2 \times \dots \times n_r$ , the Local Unitary (LU) group,  $G = U(n_1) \otimes \dots \otimes U(n_r)$  acts on  $\mathfrak{P}_+$  in non-transitive way. This circumstance causes a stratification of  $\mathfrak{P}_+$ , reflecting a diversity of non-local properties the system exposes. Classes of the equivalence with respect to the LU transformations form the so-called entanglement space, the factor space:

$$\mathcal{E} = \frac{\text{Space of states}}{\text{Group of LU transformations}}.$$

Thus characterization and classification of a quantum system non-locality reduces mainly to a classical mathematical problem - description of the orbit space of compact Lie groups.

## 2 Recipe for the orbit space description

The orbit space of a compact Lie group action on a linear space can be described in the framework of the invariant theory within the direction initiated by Processi and Schwarz [1, 2].

Consider the compact Lie group  $G$  acting linearly on the real  $d$ -dimensional vector space  $V$  and let  $\mathbb{R}[V]^G$  is the corresponding ring of the  $G$ -invariant polynomials on  $V$ . Assume  $\mathcal{P} = (p_1, p_2, \dots, p_q)$  is a set of homogeneous polynomials that form the integrity basis,  $\mathbb{R}[x_1, x_2, \dots, x_d]^G = \mathbb{R}[p_1, p_2, \dots, p_q]$ . Elements of the integrity basis define the polynomial mapping:

$$p: V \rightarrow \mathbb{R}^q; \quad (x_1, x_2, \dots, x_d) \rightarrow (p_1, p_2, \dots, p_q).$$

Since  $p$  is constant on the orbits of  $G$  it induces a homeomorphism of the orbit space  $V/G$  and the image  $X$  of  $p$ -mapping;  $V/G \simeq X$  [3]. In order to describe  $X$  in terms of  $\mathcal{P}$  uniquely, it is necessary to take into account the *syzygy ideal* of  $\mathcal{P}$ , i.e.,

$$I_{\mathcal{P}} = \{h \in \mathbb{R}[y_1, y_2, \dots, y_q] : h(p_1, p_2, \dots, p_q) = 0, \text{ in } \mathbb{R}[V]\}.$$

Let  $Z \subseteq \mathbb{R}^q$  denote the locus of common zeros of all elements of  $I_{\mathcal{P}}$ , then  $Z$  is algebraic subset of  $\mathbb{R}^q$  such that  $X \subseteq Z$ . Denoting by  $\mathbb{R}[Z]$  the restriction of  $\mathbb{R}[y_1, y_2, \dots, y_q]$  to  $Z$  one can easily verify that  $\mathbb{R}[Z]$  is isomorphic to the quotient  $\mathbb{R}[y_1, y_2, \dots, y_q]/I_{\mathcal{P}}$  and thus  $\mathbb{R}[Z] \simeq \mathbb{R}[V]^G$ . Therefore the subset  $Z$  essentially is determined by  $\mathbb{R}[V]^G$ , but to describe  $X$  the further steps are required. According to [1, 2] the necessary information on  $X$  is encoded in the structure of  $q \times q$  matrix with elements given by the inner products of gradients,  $\text{grad}(p_i)$ :

$$\|\text{Grad}\|_{ij} = (\text{grad}(p_i), \text{grad}(p_j)) .$$

Summarizing these observations, the orbit space is identified with the semi-algebraic variety, defined as points, satisfying two conditions:

- a)  $z \in Z$ , where  $Z$  is the surface defined by the syzygy ideal for the integrity basis of  $\mathbb{R}[V]^G$ ;
- b)  $\text{Grad}(z) \geq 0$ .

### 3 Describing the entanglement space $\mathcal{E}_2$

The general scheme sketched above has been applied to the analyzes of a 4-dimensional bipartite quantum system with partition,  $n_1 = n_2 = 2$ , i.e., a pair of qubits.

To make Procesi-Schwarz method applicable we linearize at first the adjoint action of  $U(2) \otimes U(2)$  group on the space  $\mathcal{H}_{4 \times 4}$  of  $4 \times 4$  Hermitian matrices:

$$(\text{Ad } g)\varrho = g \varrho g^{-1}, \quad g \in U(2) \otimes U(2), \quad (1)$$

by the mapping  $\mathcal{H}_{4 \times 4} \rightarrow \mathbb{R}^{16}$ ;  $\varrho \rightarrow \mathbf{v} = (v_1, v_2, \dots, v_{16})$  and considering on  $\mathbb{R}^{16}$  the linear representation

$$\mathbf{v}' = L\mathbf{v}, \quad L \in U(2) \otimes U(2) \otimes \overline{U(2) \otimes U(2)},$$

where a line over expression means the complex conjugation. Further using the integrity basis for  $\mathbb{R}[\mathbf{v}]^{U(2) \otimes U(2)}$ , suggested in [4]-[7] one can pass to the analysis of the semi-positivity of the Grad-matrix and determine the set of inequalities defining the orbit space  $\mathbb{R}^{16}/U(2) \otimes U(2)$ . However, this is not the end of a story. The orbit space defined in this manner is not the space of entanglement, namely  $\mathcal{E}_2 \subseteq \mathbb{R}^{16}/U(2) \otimes U(2)$ . Indeed, due to the non-negativity of density matrices the space of physical states is  $\mathfrak{P}_+ \subset \mathbb{R}^{15}$  defining by a further set of constraints on elements of integrity basis (see e.g. [7]). Concluding it is worth to stress that analysis of the relevant geometry of  $\mathcal{E}_2$ , determining via a complete set of polynomial inequalities in LU invariants, including both, mentioned here, as well as arising from the semi-positivity conditions on the density matrix of 2-qubits, represents a non-trivial mathematical problem and has highly important consequences for quantum information theory and quantum computing.

### 4 Computational issues

To derive the inequalities in the LU invariants determining the orbit space  $\mathbb{R}^{16}/U(2) \otimes U(2)$ , one has first to express the entries of Grad-matrix in terms of the invariants and then compute its Smith normal form. For the last computation we are going to try recent algorithms [8] and their implementation in Maple. Unlike all previously known algorithms for reduction of a matrix to the Smith normal form, the algorithms of paper [8] may work when the entries of a matrix are multivariate polynomials. The ring of such polynomials is not Euclidean (i.e., not principal ideal) domain that is at the basis of all other algorithms.

### References

- [1] C. Procesi and G. Schwarz, The geometry of orbit spaces and gauge symmetry breaking in supersymmetric gauge theories, Phys. Lett. **B 161**, 117-121 (1985).
- [2] C. Procesi and G. Schwarz, Inequalities defining orbit spaces, Invent.math. **81** 539-554 (1985).
- [3] D. Cox, J. Little and D. O'Shea, Ideals, Varieties, and Algorithms, Third Edition, Springer, (2007).



- [4] C. Quesne,  $SU(2) \otimes SU(2)$  scalars in the enveloping algebra of  $SU(4)$ , *J. Math. Phys.* **17** 1452–1467 (1976).
- [5] M. Grassl, M. Rotteler and T. Beth, Computing local invariants of qubit quantum systems, *Phys. Rev. A* **58**, 1833-1839 (1998).
- [6] R. C. King, T. A. Welsh and P D Jarvis, The mixed two-qubit system and the structure of its ring of local invariants, *J. Phys. A: Math. Theor.* **40** 10083-10108 (2007).
- [7] V. Gerdt, A. Khvedelidze and Yu. Pali, On the ring of local polynomial invariants for a pair of entangled qubits, *Zapiski POMI* **373**, 104-123 (2009).
- [8] M.S. Boudellioua, Computation of the Smith Form for Multivariate Polynomial Matrices Using Maple, *American Journal of Computational Mathematics* **2**, 21-26 (2012).

# Mathematica Package *QuantumCircuit* for Simulation of Quantum Computation

V.P. Gerdt

Joint Institute for Nuclear Research, Dubna, Russia

A.N. Prokopenya

Warsaw University of Life Sciences - SGGW, Warsaw, Poland

`alexander_prokopenya@sggw.pl`

## Abstract

In papers [1, 2, 3] we presented our Mathematica package *QuantumCircuit* for simulation of quantum computation based on the circuit model [4]. The package provides a user-friendly interface to specify a quantum circuit, to draw it, and to construct the corresponding unitary matrix for quantum computation defined by the circuit. Using this matrix, one can find the final state of the quantum memory register by its given initial state and to check the operation of the algorithm determined by the quantum circuit.

Here we present an application of the package *QuantumCircuit* to simulation of quantum circuits implementing such well-known quantum algorithm as the Shor algorithm for integer factorization. Besides, we analyze some examples of the circuits used for quantum error correction and entanglement simulation. The main purpose of the talk is to demonstrate that a proper extension of such powerful software system as Mathematica in order to simulate quantum circuits helps to better understanding of fundamental and applied aspects of quantum computation.

## Keywords

Quantum computation, Mathematica simulator, circuit model, quantum algorithms, quantum error correction, entanglement

## References

- [1] V. P. Gerdt, R. Kragler, A. N. Prokopenya. A Mathematica Package for Simulation of Quantum Computation. *Computer Algebra in Scientific Computing CASC2009*, LNCS 5743, Springer (2009) pp. 106–117.
- [2] V. P. Gerdt, A. N. Prokopenya. Some Algorithms for Calculating Unitary Matrices for Quantum Circuits. *Programming and Computer Software*, 36 (2010) 111–116.
- [3] V. P. Gerdt, A. N. Prokopenya. The circuit model of quantum computation and its simulation with Mathematica. *Mathematical Modeling and Computational Science MMCP2012*, LNCS 7125, Springer (2012) pp. 43–55.
- [4] M. Nielsen, I. Chuang *Quantum Computation and Quantum Information*, Cambridge University Press (2000).

# Simulating quantum computers with Mathematica: QDENSITY *et al.*

Bruno Julia-Diaz  
University of Barcelona (Spain)

Frank Tabakin  
University of Pittsburgh (USA)

`bruno@ecm.ub.edu`

## Abstract

Symbolic algebra packages, such as Mathematica, provide a versatile framework to study a number of problems in quantum mechanics. They are particularly suited to study quantum problems where only a small number of qubits participate. We will describe the main ingredients of our Mathematica packages, QDENSITY [1] and QCWAVE [2], which can be used to simulate a number of well-known quantum circuits such as teleportation circuits, Grover's search algorithms and others. Applications to quantum correction circuits and cluster state quantum computation will be outlined.

[1] QDENSITY, A Mathematica Quantum Computer simulation, B. Julia-Diaz, J. M. Burdis, and F. Tabakin, *Comp. Phys. Comms*, 174, 914 (2005).

[2] QCWAVE, a Mathematica quantum computer simulation update, F. Tabakin, B. Julia-Diaz, *Comp. Phys. Comm.* 182 (2011) 1693.

## Keywords

quantum simulation, Mathematica, quantum circuits

# Functional framework for representing and transforming quantum channels

Jarosław Adam Mischczak  
Institute of Theoretical and Applied Informatics,  
Polish Academy of Sciences  
Bałtycka 5, 44-100 Gliwice, Poland

`mischczak@iitis.pl`

## Abstract

We develop a framework which aims to simplify the analysis of quantum states and quantum operations by harnessing the potential of function programming paradigm. We show that the introduced framework allows a seamless manipulation of quantum channels, in particular to convert between different representations of quantum channels, and thus that the use of functional programming concepts facilitates the manipulation of abstract objects used in the language of quantum theory.

For the purpose of our presentation we will use *Mathematica* computer algebra system. This choice is motivated twofold. First, it offers a rich programming language based on the functional paradigm. Second, this programming language is combined with powerful symbolic and numeric manipulation capabilities.

## Keywords

quantum channels, functional programming, scientific computing

## 1 Introduction

Functional programming is frequently seen as an attractive alternative to the traditional methods used in scientific computing, which are based mainly on the imperative programming paradigm [3]. Among the features of functional languages which make them suitable for the use in this area is the easiness of execution of the functional code in the parallel environments.

The main aim of this work is to show that the functional programming concepts facilitate the use of abstract objects used in the language of quantum theory. We develop a framework which aims to simplify the analysis of quantum states and quantum operations by harnessing the potential of functional programming paradigm. For the purpose of our presentation we will use *Mathematica* computer algebra system. This choice is motivated twofold. First, it offers a rich programming language based on the functional paradigm. Second, this programming language is combined with powerful symbolic and numeric manipulation capabilities.

During the last few years a number of simulators of quantum information processing has been developed using *Mathematica* computing system [8, 5, 7, 2]. Unfortunately, these packages do not use functional programming capabilities of this system and are focused on pure states and unitary operations. Moreover, they focus on the quantum mechanical systems which can be represented using state vectors and include only a basic functionality required for the purpose of manipulating and analyzing quantum states.

In this paper we follow the pragmatic approach and we provide a set of useful constructions which can be helpful for the analysis of quantum channels. At the same time we advocate the use of functional programming in this approach. We argue that by using the functional language elements provided by *Mathematica* one can easily and efficiently convert between different representations of quantum channels.

## 2 Functional syntax for quantum channels

### 2.1 Notation

In the following we assume that the quantum systems are represented by finite-dimensional density matrices, *i.e.* positive semidefinite complex matrices with unit trace. The space of density matrices of dimension  $d$  is denoted by  $\Omega_d$ . We use **res**, **unres** operations [6] for converting between matrix and vector forms of states and operators. In the *Mathematica* language function **res** is defined as a synonym for a built-in function **Flatten**

```
Res = Function[m, Flatten[m]];
```

This function transforms a matrix  $m$  into a vector in a row order. Function **unres**, which is a reverse transformation, is defined in *Mathematica* as

```
Unres = Function[m, Partition[m, Sqrt[Length[m]]]];
```

and it uses built-in function **Partition** to get back from a one-dimensional list to a matrix. As the space of density matrices is unitary with Hilbert-Schmidt scalar product, we introduce a function

```
HSInner = Function[x, Function[y, Tr[x.ConjugateTranspose[y]]]];
```

which, thanks to the curried form, allows using a partial application in the application of this scalar product.

Unfortunately *Mathematica* does not provide a straightforward support for the partial application of functions. The language does not allow using functions with too few parameters and one has to explicitly use empty slots (#-signs) to define a partially applied function. For this reason in order to use the functional version of some procedures, it is necessary to provide a curried version of these functions.

### 2.2 Simple channels

Let us illustrate the above considerations with the simplest example – the transposition map. This map is defined as

$$\rho \mapsto \rho^T, \quad (1)$$

and can be expressed in *Mathematica* as

```
trans = Function[x, Transpose[x]]
```

or using more compact syntax as `trans = Transpose[#]&`.

One should note that this map is not completely positive, hence it does not represent a valid quantum channel. Nevertheless, it is useful for presenting basic transformations which can be performed on quantum channels.

If we would like to apply this function on some state  $\rho$  we simply write `trans[ $\rho$ ]`. In many situations however, one needs to apply a map on a list `rhos` of states or matrices. In this case we simply map the functions representing the map on the list using **Map** function as

```
Map[trans, rhos]
```

or using more compact syntax as `trans /@ rhos`.

### 2.3 Channels with parameters

In order to use channels defined by parametrized expression, one can employ partially applied functions. The simplest example of such channels is a depolarizing channel  $\Psi_{D(p,d)}$  defined as

$$\Psi_{D(p,d)}(\rho) = (1-p)\rho + p\frac{1}{n}\mathbb{1}_n, \quad (2)$$

where we assume that  $\rho \in \mathbb{M}_n$  and  $\mathbb{1}_n$  denotes the identity matrix of the appropriate size.

Using the notation introduced in Section ??, this channel can be represented by a function

```
dep = Function[d, Function[p, Function[x,  
  (1-p)x + p IdentityMatrix[d]/d  
]]];
```

Here we follow the convention that the function parameters should be organized in such a way, that by providing all but one of them, we obtain a function accepting quantum state as an argument. In the above case the first two parameters represent the dimension and the reliability of the channel (the probability of introducing no errors).

Function `dep` requires three arguments and its application on state  $\rho$  is achieved by first declaring the instance of the channel for a fixed dimension (*e.g*  $d=4$ )

```
dep4 = dep[4];
```

and next using this function with a specific probability  $p$

```
dep4[p][ $\rho$ ];
```

However, one can use `dep` function to define the expression in which only two arguments are provided

```
g = (dep[#1][p][#2]) &
```

and this allows obtaining a general definition of the depolarizing channel with a fixed parameter  $p$ , identical to the following definition

```
Function[d, Function[x, (1-p) x + p IdentityMatrix[d]/d]];
```

Function  $g$  accepts two arguments representing the dimension and the input state. Its application on some state  $\rho \in \mathbb{M}_4$  reads

```
g[4][ $\rho$ ];
```

and this syntax allows the selection of an argument which should be fixed during the manipulation.

### 3 Representations of quantum channels

#### 3.1 Natural representation

As channels are linear mappings, it is possible, at least in finite-dimensional case, to represent them by matrices. Let us assume that we are dealing with  $d = n \times n$  dimensional matrices.

The base in  $n^2$ -dimensional space  $\mathbb{M}_n$  is given by matrices, which can be obtained by using `Unres` operations on the base vectors in the  $d$ -dimensional space  $\mathbb{C}^d, d = n^2$ , as

```
base = Map[Unres[UnitVector[d, #]] &, Range[d]];
```

where `Range[d]` returns a list containing numbers  $1, 2, \dots, d$ . In the following we assume that the  $d$ -dimensional matrix base can be obtained using function `BaseMatrices[d]` defined as

```
BaseMatrices = Function[d, Map[Unres[UnitVector[d, #]] &, Range[d]]];
```

If the list `fBase` contains the images of the quantum channel  $f$  on the base

```
fBase = f /@ base
```

then the natural representation can be calculated by unreshaping the images of the map on the base matrices in  $\mathbb{M}_{d^2}$ ,

```
{Res /@ fBase}
```

Combining this into one function gives

```
NaturalRepresentation = Function[f, Function[d,
  With[{base=BaseMatrices[d^2]}, Map[Res[f[#]]&, base]]
];
```

We denote the natural representation of the channel  $\Phi$  by  $\mathcal{M}_\Phi$ , assuming that this matrix is obtained in the standard basis. Matrix  $\mathcal{M}_\Phi$  is sometimes called a supermatrix for the channel  $\Phi$ .

The above considerations can be summarized as the following definition.

**Definition 1 (Natural representation)** *For a given channel  $\Psi$ , the natural representation of  $\Phi$  by  $\mathcal{M}_\Phi$  is defined as*

$$(\mathcal{M}_\Phi)_i = \mathbf{res} \Phi(b_i) \quad (3)$$

where  $(A)_i$  denotes  $i$ -th column of the matrix  $A$  and  $b_i, i = 1, n^2$  denotes base matrices in  $\mathbb{M}_n$ .

For example, in order to obtain the matrix representation of the depolarizing channel `dep` acting on one qubit, one should use `NaturalRepresentation` function as

```
NaturalRepresentation[dep][2][p][2]
```

In a similar manner one can check that the natural representation of the one-qubit transposition channel `trans`

```
NaturalRepresentation[trans][2]
```

is equal to the SWAP gate.

### 3.2 General natural representation

Clearly one can represent a given channel in a matrix form using not only a canonical base, but any orthonormal basis in  $\mathbb{C}^{n^2}$ . In this situation one cannot use the method described above as it relies on the special form of the canonical base matrices.

The straightforward method of calculating a matrix representation, is based on the formula

$$(M_{\Phi}^b)_{ij} = \text{tr}[b_i \Phi(b_j)^\dagger], \quad (4)$$

where  $b_i, i = 1, \dots, n^2$  denotes the base.

**Definition 2 (General natural representation)** *For a given channel  $\Psi$ , the general natural representation of  $\Phi$  in base  $b$  is defined as*

$$(\mathcal{M}_{\Phi}^b)_{ij} = \text{tr}[\Phi(b_i) b_j^\dagger], \quad (5)$$

where  $b_i, i = 1, n^2$  denote base matrices in  $\mathbb{M}_n$ .

This definition can be implemented using `Outer` function as

```
Function[f, Function[b,
  Outer[HSInner[#1][#2]&, Map[f,b], b, 1]
]];
```

where `base` is a given base or, alternatively, by using `Map` function as

```
Function[f, Function[b,
  Map[Map[#, b] &, Map[HSInner, Map[f, b]]]
]];
```

This method requires  $n^4$  multiplications of  $n \times n$  matrices and is highly inefficient.

The simplest method is to reconstruct a change of basis matrix  $M_B$ ,

```
 $M_B = \text{Map}[\text{Res}, b]$ 
```

and use it to obtain  $M_{\Phi}^b$  as

$$M_{\Phi}^b = M_B M_{\Phi} M_B^\dagger. \quad (6)$$

### 3.3 Choi-Jamiolkowski representation

Complete positivity, one of the requirements for the map between finite-dimensional spaces can be formulated using Choi-Jamiolkowski representation of a map [4, 1]. This representation in the context of quantum channels is known as Jamiolkowski isomorphism and here the image of this isomorphism is denoted as  $\mathcal{J}_{\Phi}$ .

The Choi-Jamiolkowski representation is closely related to the natural representation. The natural representation of the channel acting on  $n \times n$ -dimensional matrices is always obtained with respect to some bases  $\{b_i\}_{i=1, n^2}$ , where  $n^2$  is the dimension of the state space.

If one uses base  $b_i$  to obtain the natural representation of the channel  $\Phi$  resulting in matrix  $M_{\Phi}^b$ , then the Choi-Jamiolkowski matrix for this channel is obtained as

$$\{\mathcal{J}_{\Phi}^b\}_{i,j} = \text{tr}[M_{\Phi}^b(b_i \otimes b_j)], \quad (7)$$

for  $i, j = 1, n^2$ .

**Definition 3 (Choi-Jamiolkowski matrix)** Let  $\{b_i\}$  be a base in  $\mathbb{C}^{n^2}$ . The Choi-Jamiolkowski matrix corresponding to a general natural representation in base  $\{b_i\}$  is defined as

$$\{\mathcal{J}_\Phi^b\}_{i,j} = \text{tr}[M_\Phi^b(b_i \otimes b_j)]. \quad (8)$$

The Choi-Jamiolkowski representation of the channel  $\Phi$  can be also obtained using several other methods. One of the simplest formulas is the one expressing  $\mathcal{J}_\Phi$  as a sum

$$\mathcal{J}_\Phi = \sum_{i=1}^d \Phi(e_i) \otimes e_i. \quad (9)$$

Assuming that base represents matrix base in  $d$ -dimensional space, this representation can be used by mapping

```
cjBase = Map[KroneckerProduct[f[#], #] &, base]
```

and accumulating the results

```
Plus /@ cjBase
```

Combining the above into one function gives

```
ChoiJamiolkowskiRepresentation = Function[f, Function[d,
  With[{base=BaseMatrices[d]},
    Map[Plus, [Map[KroneckerProduct[f[#], #] &, base]]]
  ]];
```

The Choi-Jamiolkowski representation of a channel is related to the natural representation, one can easily construct a Choi-Jamiolkowski matrix corresponding to a given generalized natural representation.

**Acknowledgements** This work was supported by the Polish Ministry of Science and Higher Education under the grant number IP2011 036371 and by the Polish National Science Centre under the grant number DEC-2011/03/D/ST6/00413. Author would like to acknowledge stimulating discussions with Z. Puchała, P. Gawron, D. Kurzyk, V. Jagadish and P. Zawadzki.

## References

- [1] M.-D. Choi. Completely positive linear maps on complex matrices. *Linear Algebr. Appl.*, 10(3):285–290, 1975.
- [2] J. L. Gómez-Muñoz and F. Delgado-Cepeda. Quantum 2.3 for Mathematica 8, 2011-. Software available on-line at <http://homepage.cem.itesm.mx/lgomez/>.
- [3] K. Hinsien. The promises of functional programming. *Comput. Sci. Eng.*, 11(4):86–90, 2009.
- [4] A. Jamiolkowski. Linear transformations which preserve trace and positive semidefiniteness of operators. *Rep. Math. Phys.*, 3(4):275–278, 1972.
- [5] B. Juliá-Díaz, J.M. Burdis, and F. Tabakin. QDENSITY—a Mathematica quantum computer simulation. *Comput. Phys. Commun.*, 174(11):914934, 2006.
- [6] J.A. Miszczak. Singular value decomposition and matrix reorderings in quantum information theory. *Int. J. Mod. Phys. C*, 22(9):897–918, 2011.
- [7] F. Tabakin and B. Juliá-Díaz. QCWAVE – a Mathematica quantum computer simulation update. *Comput. Phys. Commun.*, 182(8):16931707, 2011.
- [8] H. Touchette and P. Dumais. The quantum computation package for Mathematica 4.0. Software available on-line at <http://crypto.cs.mcgill.ca/QuCalc/>, 2000-.



# Ultimate limits to squeezing of quantum fluctuations

Arkadiusz Orłowski

Warsaw University of Life Sciences - SGGW (Poland)

arkadiusz\_orlowski@sggw.pl

## Abstract

Various limits to squeezing of quantum fluctuations below the vacuum level (still being a hot topic in such areas as detection of gravitational waves via high-precision optical interferometry, quantum non-demolition measurements, high-resolution spectroscopy, and low-noise optical communication systems) are analyzed and discussed.

Problems related to the optimum level of the above-mentioned quantum noise reduction for finite superpositions of orthonormal basis-states of quantum harmonic oscillator are thoroughly investigated. An explicit construction of states leading to maximum degree of squeezing is provided and both exact and approximate expressions for minimum variances of position and momentum operators are given. Using some analytical tools offered by computer algebra software new properties of such quantum states are discovered. Possible applications of the obtained results to quantum optics and quantum information are also elaborated.

As a by-product, new interesting properties of some classic orthogonal functions, especially an interesting behavior of zeros of properly rescaled Hermite polynomials, are obtained.

## Keywords

Quantum fluctuations, squeezing, harmonic oscillators, Hermite polynomials

# Geometry and Dynamics of Algorithms on the Quantum Information Space

Yoshio Uwano

Faculty of Systems Information Science

Future University Hakodate

116-2 Kameda Nakano-cho, Hakodate 041-8655, Japan

uwano@fun.ac.jp

## Abstract

Quantum computing and quantum information are well known to be very hot interdisciplinary fields, where a number of approaches have been taken. Among those, geometric methods are known to be of good use. This short paper is a direct continuation of a paper by the author [Y.Uwano, *Search Algorithms for Engineering Optimization* (T.Abrão ed., In-Tech Press, Rijeka, 2013), pp.261-284] on a geometric study on the Grover-type search for an ordered tuple of multi-qubits: A classification of geodesics in the space of ordered tuples of multi-qubits is made according to which of those reduce to the geodesics in the quantum information space with respect to the mixture, the exponential and the Levi-Civita parallel transports. Computer algebra applicability to this problem is mentioned of also from the view point of matrix algebra.

## Keywords

Quantum information space, Geodesics, Search algorithm

## 1 Introduction

Quantum computing and quantum information have been a pair of the most challenging research subjects [1] in recent decades, to which a number of disciplines have been applied. From geometry viewpoint, the work of Miyake and Wadati [2] in 2001 is well known which provides a clear geometric characterization of Grover's celebrated search algorithm for a single target [3]: In the paper [2], the Grover search sequence in  $2^n$  data is shown to be on a geodesic in  $(2^{n+1} - 1)$ -dimensional sphere  $S^{2^{n+1}-1}$ . Further, through a geometric reduction of  $S^{2^{n+1}-1}$  to the complex projective space  $\mathbf{CP}^{2^n-1}$ , the search sequence is projected to a sequence in  $\mathbf{CP}^{2^n-1}$ , that is shown to be on a geodesic in  $\mathbf{CP}^{2^n-1}$ .

Motivated by the paper [2], the author constructed a Grover-type search algorithm for an ordered tuple of multi-qubits [4]. A geometric reduction different from that in [2] is applied to the extended space of ordered tuples of multi-qubits (ESOT),

$$M_1(2^n, \ell) = \{\Phi \in M(2^n, \ell) \mid \frac{1}{\ell} \text{trace } \Phi^\dagger \Phi = 1\}, \quad (1)$$

where  $M(2^n, \ell)$  denotes the set of  $2^n \times \ell$  complex matrices and  $^\dagger$  stands for the adjoint operation. The geometric reduction in [4] is made through the projection

$$\pi^{(n, \ell)} : \Phi \in M_1(2^n, \ell) \mapsto \frac{1}{\ell} \Phi^\dagger \Phi \in P_\ell \quad (2)$$

with

$$P_\ell = \{\rho \in M(\ell, \ell) \mid \rho : \text{positive semidefinite, } \rho^\dagger = \rho, \text{ trace } \rho = 1\}, \quad (3)$$

where  $M(\ell, \ell)$  denotes the set of  $\ell \times \ell$  complex matrices. The  $P_\ell$  is well known to be the space of density matrices of degree- $\ell$ , which plays a central role in quantum information theory [5]. Through the reduction process, the QIS can be endowed with a Riemannian metric that makes the projection  $\pi^{(n, \ell)}$  a Riemannian submersion. Surprisingly, the Riemannian metric thus endowed

is shown to coincide with the SLD-Fisher metric up to a constant multiple [4], so that the QIS with the SLD-Fisher metric is obtained as a natural outcome of the ESOT with the standard Riemannian metric through the geometric reduction.

A geometric characterization of the Grover-type search sequence in the ESOT and its reduction in the QIS is made in another paper [6] by the author, where geodesics in the ESOT/QIS are defined as autoparallel curves with respect to parallel transports fixed to the ESOT/QIS, respectively. It is shown in [6] that the search sequence in the ESOT is on a geodesic with respect to the Levi-Civita parallel transport for the standard metric and that the reduced search sequence in the QIS is on a geodesic with respect to the mixture parallel transport. Since three parallel transports, viz the mixture (m-), the exponential (e-) and the Levi-Civita (LC) parallel transport, in the QIS are said to be crucial in quantum information geometry [5], it is interesting to classify the geodesics in the ESOT according to which of those are reduced to the geodesics in the QIS with respect to the m-, the e- and the LC parallel transport. Note that the LC parallel transport is associated with the SLD-Fisher metric, a crucial metric in quantum information geometry.

As a direct continuation of the paper [6], this short paper aims to report briefly a classification of geodesics in the ESOT according to which of those can be reduced to the geodesics with respect to the m-parallel transport, those to the LC parallel transport and otherwise. Section 2 is a preliminary section, where the geometric reduction to be applied [4, 6] and the geodesics in the ESOT [6] are concisely reviewed. Section 3 presents the classification of the geodesics in the ESOT. In subsection 3.1, the geodesics in the ESOT reducible to the LC geodesics in the QIS are identified. The horizontal condition given in Sec. 2 for curves in the ESOT plays a key role. Subsection 3.2 deals with the geodesics in the ESOT reducible to the m-geodesics in the QIS. In contrast with subsection 3.1, the vertical condition given in Sec. 2 for tangent vectors of the QIS plays a key role. Subsection 3.3 is for concluding remarks including an applicability of computer algebra to the present classification problem.

As another application of [4], a pair of papers by the author exist on the gradient-equation realization in the QIS of the Karmarkar flow and of the Hebb-type learning equation [7, 8].

## 2 Preliminaries

We here give a very concise review of the geometric reduction of the ESOT given by (1) to the QIS given by (3). To ensure the validity of differential calculus, the regular parts of them, denoted by  $M_1(2^n, \ell)$  and  $\dot{P}_\ell$ , will be often considered also, which consist of the matrices of rank  $\ell$  in  $M_1(2^n, \ell)$  and of positive definite matrices in  $P_\ell$ , respectively (see [4, 6, 7, 8]). A key to the reduction is the (stratified) fibered manifold structure of  $M_1(2^n, \ell)$  associated with the  $U(2^n)$  action

$$\alpha_g : \Phi \in M_1(2^n, \ell) \mapsto g\Phi \in M_1(2^n, \ell) \quad (g \in U(2^n)). \quad (4)$$

Indeed, in view of  $\pi^{(n, \ell)} \circ \alpha_g = \pi^{(n, \ell)} (g \in U(2^n))$ , we have

$$\pi^{(n, \ell)} : M_1(2^n, \ell) \rightarrow P_\ell \cong U(2^n) \backslash M_1(2^n, \ell), \quad \pi^{(n, \ell)} : \dot{M}_1(2^n, \ell) \rightarrow \dot{P}_\ell \cong U(2^n) \backslash \dot{M}_1(2^n, \ell). \quad (5)$$

In particular, the latter in (5) implies that  $\dot{M}_1(2^n, \ell)$  admits the fibered manifold structure over  $\dot{P}_\ell$  with the fiber  $U(2^n)/U(2^n - \ell)$ , where  $U(2^n - \ell)$  stands for the group of unitary matrices of degree  $2^n - \ell$ . From now on, we focus our attention to the whole spaces,  $M_1(2^n, \ell)$  and  $P_\ell$ , without mentioning of the handling of irregular points due to the page length limitation.

The fibered structures (5) lead us to the direct-sum decomposition of the tangent space,

$$T_\Phi M_1(2^n, \ell) = \{X \in M(2^n, \ell) \mid \frac{1}{\ell} \Re(\text{trace } \Phi^\dagger X) = 0\} \quad (\Phi \in M_1(2^n, \ell)), \quad (6)$$

of  $M_1(2^n, \ell)$  at  $\Phi \in M_1(2^n, \ell)$ . Indeed, defining the *vertical* subspace by

$$\text{Ver}(\Phi) = \{X \in T_\Phi M_1(2^n, \ell) \mid X = \zeta \Phi, \zeta \in u(2^n)\} \quad (7)$$

with  $u(2^n)$  consisting of the anti-Hermitian matrices of degree  $2^n$ , we have

$$T_\Phi M_1(2^n, \ell) = \text{Ver}(\Phi) \oplus \text{Hor}(\Phi) \quad (\Phi \in M_1(2^n, \ell)), \quad (8)$$

where  $\text{Hor}(\Phi)$  is the complementary subspace orthogonal to  $\text{Ver}(\Phi)$  with respect to the canonical Riemannian metric

$$((X, X'))_\Phi^{ESOT} = \frac{1}{\ell} \Re(\text{trace } X^\dagger X') \quad (X, X' \in T_\Phi M_1(2^n, \ell), \Phi \in M_1(2^n, \ell)). \quad (9)$$

According to the direct-sum decomposition (8), we define the horizontal lift of any tangent vector  $\Xi \in T_\rho P_\ell$ .

**Definition 2.1.** *The horizontal lift of a tangent vector  $\Xi$  at  $\rho \in P_\ell$  is the unique tangent vector  $\Xi^*$  at  $\Phi \in M_1(2^n, \ell)$  with  $\pi^{(n,l)}(\Phi) = \rho$  which satisfies*

$$\Xi^* \in \text{Hor}(\Phi), \quad \pi_{*,\Phi}^{(n,l)}(\Xi^*) = \Xi, \quad (10)$$

where  $\pi_{*,\Phi}^{(n,l)}$  is the differential map of  $\pi^{(n,l)}$  at  $\Phi$ .

The SLD-Fisher metric  $((\cdot, \cdot))^{QF}$  is shown to be the Riemannian metric of the QIS that makes the projection  $\pi^{(n,l)}$  the Riemannian submersion in the sense [4, 9],

$$((\Xi, \Xi'))_\rho^{QF} = 4((\Xi^*, (\Xi')^*))_\Phi^{ESOT} \quad (\Xi, \Xi' \in T_\rho P_\ell, \pi^{(n,l)}(\Phi) = \rho). \quad (11)$$

We give a pair of lemmas and a definition convenient to the succeeding sections.

**Lemma 2.2.** *A tangent vector  $X \in T_\Phi M_1(2^n, \ell)$  ( $\Phi \in M_1(2^n, \ell)$ ) is horizontal, viz  $X \in \text{Hor}(\Phi)$ , if and only if it satisfies*

$$\Phi X^\dagger - X \Phi^\dagger = 0. \quad (12)$$

**Lemma 2.3.** *A tangent vector  $X \in T_\Phi M_1(2^n, \ell)$  ( $\Phi \in M_1(2^n, \ell)$ ) is vertical, viz  $X \in \text{Ver}(\Phi)$ , if and only if it satisfies*

$$\pi_{*,\Phi}^{(n,l)}(X) = \Phi^\dagger X + X \Phi^\dagger = 0. \quad (13)$$

**Definition 2.4.** *A smooth curve  $\Gamma = \{\gamma(t) \in M_1(2^n, \ell) \mid t \in \exists[a, b]\}$  ( $\gamma: C^\infty$  function) in  $M_1(2^n, \ell)$  is horizontal if and only if it satisfies  $\frac{d\gamma}{dt}(t) \in \text{Hor}(\gamma(t))$  for any  $t \in [a, b]$ .*

We move to describe the geodesics with respect to the Levi-Civita parallel transport (the LC geodesics) in the ESOT in an explicit form. Since the Riemannian metric  $((\cdot, \cdot))^{ESOT}$  is equal to the canonical one up to the constant multiple  $\frac{1}{2}$  (see (9)), we easily see that loci of any LC geodesic in the ESOT is a ‘great circle’, so that we have the following.

**Lemma 2.5.** *Any LC geodesic in the ESOT drawing a great circle is expressed as*

$$\Phi(s) = \Phi_0 \cos s + X_0 \sin s \quad (s \in [0, 2\pi]), \quad (14)$$

where  $s$  is the arc-length parameter and  $\Phi_0, X_0 \in M_1(2^n, \ell)$ .

We note here that  $\Phi_0$  and  $X_0$  provide the initial condition,  $\Phi(0) = \Phi_0$  and  $\frac{d\Phi}{ds}(0) = X_0$ , where the norm,  $\sqrt{((X_0, X_0))_{\Phi_0}^{ESOT}}$ , has to be fixed to be 1 under the arc length description. Which geodesic is the Grover-type search sequence is on? It is realized as (14) with

$$(\Phi_0)_{jk} = \sqrt{\frac{1}{2^n}} \begin{pmatrix} j = 1, 2, \dots, 2^n \\ k = 1, 2, \dots, \ell \end{pmatrix}, \quad X_0 = \sqrt{\frac{1}{2^n - 1}} \Phi_0 + \sqrt{\frac{2^n}{2^n - 1}} W, \quad (15)$$

where  $W$  is the target for search (see [4, 6] for detail).

### 3 Classification of geodesics

We classify the geodesics in the ESOT according to which of those can be reduced to the geodesics with respect to the m-parallel transport, those to the LC parallel transport and otherwise.

#### 3.1 Geodesics in the ESOT reducible to the LC geodesics in the QIS

We seek the geodesics in the ESOT reducible to the geodesics in the QIS with respect to the Levi-Civita parallel transport for the SLD-Fisher metric (the LC geodesics). We have the following.

**Theorem 3.1.** *A geodesic  $\Phi(s)$  in the ESOT is reduced to an LC geodesic in the QIS for the SLD-Fisher metric if and only if it is horizontal. The condition for a geodesic  $\Phi(s)$  in the ESOT to be horizontal is written in the form,*

$$\Phi_0 X_0^\dagger - X_0 \Phi_0^\dagger = 0, \quad (16)$$

in terms of the initial condition,  $\Phi(0) = \Phi_0$  and  $\frac{d\Phi}{ds}(0) = X_0$ , for  $\Phi(s)$ .

We will give a brief intuitive sketch of a proof only without getting into detail due to page length limitation. A key is the so-called ‘shortest path property’ valid for the LC geodesics [9]. Let us start with an LC geodesic of (14) not necessarily horizontal. For any sufficiently small segment  $\Sigma_{a,b}$  of the geodesic corresponding to the interval  $[a, b] (\subset [0, 2\pi])$  of  $s$ , we have the following relation between the arc-length  $L(\Sigma)$  of  $\Sigma$  and that of the reduced curve  $\pi^{(n,l)}(\Sigma)$  denoted by  $L(\pi^{(n,l)}(\Sigma))$ : On recalling (11), we have

$$\begin{aligned} L(\Sigma) &= \int_a^b \left( \left( \frac{d\Phi}{ds}, \frac{d\Phi}{ds} \right)_{\Phi(s)}^{ESOT} \right) ds \\ &= \int_a^b \left( \left( \frac{d\Phi^H}{ds}, \frac{d\Phi^H}{ds} \right)_{\Phi(s)}^{ESOT} \right) ds + \int_a^b \left( \left( \frac{d\Phi^V}{ds}, \frac{d\Phi^V}{ds} \right)_{\Phi(s)}^{ESOT} \right) ds \\ &\geq \frac{1}{4} \int_a^b \left( \left( \frac{d}{ds}(\pi^{(n,l)}(\Phi)), \frac{d}{ds}(\pi^{(n,l)}(\Phi)) \right)_{\pi^{(n,l)}(\Phi(s)}}^{QF} \right) ds = L(\pi^{(n,l)}(\Sigma)), \end{aligned} \quad (17)$$

where  $\frac{d\Phi^H}{ds}$  and  $\frac{d\Phi^V}{ds}$  are the horizontal and the vertical components of tangent vector  $\frac{d\Phi}{ds}(s)$  according to the direct-sum decomposition (8). Since the equality holds true on the third line of (17) only for the horizontal geodesics, the reduced segment  $\pi^{(n,l)}(\Sigma)$  becomes shortest if  $\Sigma$  is a segment of a horizontal geodesic.

### 3.2 Geodesics in the ESOT reducible to the m-geodesics in the QIS

This subsection is devoted to report another class of geodesics in the ESOT that is characterized to be reduced to the m-geodesics, the geodesics with respect to the mixture parallel transport, in the QIS. We start with characterizing the m-geodesics in the QIS. The geodesic, denoted by  $\rho(t)$ , from  $\rho_0 \in P_\ell$  to  $\rho_1 \in P_\ell$  is written in a very simple form [5],

$$\rho(t) = (1-t)\rho_0 + t\rho_1 \quad (t \in [0, 1]). \quad (18)$$

Note that the parameter  $t$  is chosen arbitrary up to affine transformations;  $t \rightarrow \alpha t + \beta$  ( $\alpha, \beta \in \mathbf{R}$ ). To those who are not familiar to differential geometry, the m-geodesics might be understood as ‘straight-line segments’ in the QIS. This is not true, however, since the QIS is endowed *not* with the Euclidean metric *but* with the SLD-Fisher metric which is of course not Euclidean.

In contrast with the previous subsection for the case reducible to the LC geodesics in the QIS, we are not able to utilize the shortest path property to characterize the m-geodesics since the m-parallel transport is not the Levi-Civita parallel transport for the SLD-Fisher metric of the QIS. Hence we show a minimum of calculation to reach to Theorem 3.2 below. On writing any great circle (geodesic) in the ESOT in the form (14), our task is to find a condition for  $\pi^{(n,l)}(\Phi(s))$  to be on an m-geodesic in the QIS, where  $\pi^{(n,l)}(\Phi(s))$  is brought into the form,

$$\pi^{(n,l)}(\Phi(s)) = \frac{1}{2\ell} \left\{ (\Phi_0^\dagger \Phi_0 + X_0^\dagger X_0) - (X_0^\dagger X_0 - \Phi_0^\dagger \Phi_0) \cos 2s + (\Phi_0^\dagger X_0 + X_0^\dagger \Phi_0) \sin 2s \right\}, \quad (19)$$

periodic with period  $\pi$ . To seek the condition for  $\pi^{(n,l)}(\Phi(s))$  to be brought into the form (18), it is easier to manipulate the parallelity condition given below than to handle (19) directly: Let us consider the image of the tangent vector  $\frac{d\Phi}{ds}(s)$  of the geodesic at  $\Phi(s)$  through the differential map  $\pi_{*,\Phi(s)}^{(n,l)}$ , which is calculated to be

$$\begin{aligned} \pi_{*,\Phi(s)}^{(n,l)}\left(\frac{d\Phi}{ds}(s)\right) &= \frac{d}{ds} \left( \pi^{(n,l)}(\Phi(s)) \right) \\ &= \frac{1}{\ell} \left\{ (X_0^\dagger X_0 - \Phi_0^\dagger \Phi_0) \sin 2s + (\Phi_0^\dagger X_0 + X_0^\dagger \Phi_0) \cos 2s \right\} \in T_{\pi^{(n,l)}(\Phi(s))} P_\ell. \end{aligned} \quad (20)$$

The parallelity condition is the linear dependence of  $\pi_{*,\Phi(s_1)}^{(n,l)}\left(\frac{d\Phi}{ds}(s_1)\right)$  and  $\pi_{*,\Phi(s_2)}^{(n,l)}\left(\frac{d\Phi}{ds}(s_2)\right)$  for any pair of distinct  $s_1$  and  $s_2$  in  $[0, 2\pi]$ , which is clearly equivalent to the condition for  $\pi^{(n,l)}(\Phi(s))$  to be brought into the form (18). We have the following.

**Theorem 3.2.** *A geodesic  $\Phi(s)$  in the ESOT is reduced through  $\pi^{(n,l)}$  to an  $m$ -geodesic in the QIS, if and only if it satisfies one of the following conditions.*

- (a)  $\Phi_0^\dagger X_0 + X_0^\dagger \Phi_0 = 0$  and  $X_0^\dagger X_0 - \Phi_0^\dagger \Phi_0 \neq 0$ .
- (b)  $\Phi_0^\dagger X_0 + X_0^\dagger \Phi_0 \neq 0$  and  $X_0^\dagger X_0 - \Phi_0^\dagger \Phi_0 = 0$ .
- (c)  $\lambda_1(\Phi_0^\dagger X_0 + X_0^\dagger \Phi_0) + \lambda_2(\Phi_0^\dagger X_0 + X_0^\dagger \Phi_0) = 0$  for certain non-vanishing  $\lambda_j$  ( $j = 1, 2$ ) with  $\Phi_0^\dagger X_0 + X_0^\dagger \Phi_0 = 0$  and  $X_0^\dagger X_0 - \Phi_0^\dagger \Phi_0 \neq 0$ .

The case of the Grover-type search (15) corresponds to the condition (a). What do those conditions, (a)-(c), mean? On recalling Lemma 2.3 and the expression (2.5), the vanishment,  $X_0^\dagger X_0 - \Phi_0^\dagger \Phi_0 = 0$ , is equivalent to the vertical condition (13) for the tangent vector of  $\Phi(s)$  at  $s = 0$ , and so is  $X_0^\dagger X_0 - \Phi_0^\dagger \Phi_0 = 0$  at  $s = \frac{\pi}{4}$ . The condition (c) implies a kind of parallelity condition between  $\pi_{*,\Phi(0)}^{(n,l)}(\frac{d\Phi}{ds}(0))$  and  $\pi_{*,\Phi(\frac{\pi}{4})}^{(n,l)}(\frac{d\Phi}{ds}(\frac{\pi}{4}))$ .

### 3.3 Concluding remarks

As presented in the previous subsections, we have classified the LC geodesics in the ESOT into the geodesics reducible to the LC geodesics in the QIS, those to the  $m$ -geodesics and those not reducible to either of above. The existence of LC geodesics in the ESOT reducible to the  $e$ -geodesics in the QIS is an open question still. Through the connection between the geodesics in the ESOT and the QIS given rise from our classification, we may expect that quantum information objects, e.g. the quantum estimation problem, concerning with the geodesics in the QIS can connect with quantum objects with dynamics and geometry in the ESOT. On broadening our horizon to classical information geometry, there exist interesting problems, interior point algorithms, statistical estimation, machine learning and so on, that might be expected to connect with the dynamics and geometry in the ESOT through a quantization and our classification.

What is a role of computer algebra along the direction of this paper? Though we have explicitly given the conditions for the LC geodesics in the ESOT reducible to the LC and the  $m$ -geodesics in equation form, it is very difficult to imagine a concrete form of matrices,  $\Phi_0$  and  $X_0$ , for the initial condition. Computer algebra therefore expected to work well to realize the matrices in a concrete form that might lead us to a physical implementation of geodesics in the ESOT suitable to a given problem.

## References

- [1] M.A.Nielsen, I.L.Chuang, *Quantum Computation and Quantum Information* (Cambridge U.P., Cambridge, 2000).
- [2] A.Miyake and M.Wadati, Phys. Rev. A. **64**, 042317 (2001).
- [3] L.Grover, *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing*, 212 (1996).
- [4] Y.Uwano, H.Hino H, Y.Ishiwatari, Physics of Atomic Nuclei **70**, 784 (2007).
- [5] M.Hayashi, *Quantum Information* (Springer-Verlag, Berlin, 2006).
- [6] Y.Uwano, *Search Algorithms for Engineering Optimization* (T.Abrão ed., InTech Press, Rijeka, 2013), 261.
- [7] Y.Uwano, H.Yuya, *New Trends in Quantum Information* (A.Sakaji et al eds., Aracne Editrice, Rome, 2010), 257.
- [8] Y.Uwano, H.Yuya, Far East Journal of Applied Mathematics **47**, 149(2010).
- [9] R.Montgomery, *A Tour of Subriemannian Geometries, Their Geodesics and Applications* (AMS, Providence, 2002).

---

---

# Session 10: Computer algebra in algebraic topology and its applications

---

---

Organizers:

Aniceto Murillo  
Pedro Real  
Eduardo Sáenz-de-Cabezón





# On higher dimensional cocyclic Hadamard matrices

Víctor Álvarez, José Andrés Armario, María Dolores Frau, Pedro Real  
University of Seville (Spain)

valvarez@us.es

## Abstract

Little is known about the existence of improper higher dimensional Hadamard matrices (the interested reader is referred to [4, 5, 6], the main references on the subject). Since the cocyclic framework has showed to be a promising technique for handling with planar Hadamard matrices (see [3, 1, 2] for instance), we wonder if higher dimensional cocyclic matrices might be suitable as well for looking for higher dimensional improper Hadamard matrices. In this paper we first give a method for computing a basis for  $n$ -cocycles over a finite group  $G$ , from which some different techniques for looking for higher dimensional cocyclic Hadamard matrices over  $G$  are derived. Some examples are given for illustrating these procedures.

## Keywords

Hadamard matrix, cocyclic Hadamard matrix, higher dimensional Hadamard matrix

## References

- [1] V. Álvarez, J.A. Armario, M.D. Frau and P. Real. A system of equations for describing cocyclic Hadamard matrices. *J. Comb. Des.* **16**, 276–290, (2008).
- [2] V. Álvarez, J.A. Armario, M.D. Frau and P. Real. The homological reduction method for computing cocyclic Hadamard matrices. *J. Symb. Comput.*, **44**, 558–570, (2009).
- [3] K.J. Horadam. Hadamard matrices and their applications. Princeton: Princeton University Press, (2007).
- [4] P.J. Shlichta. Three and four-dimensional Hadamard matrices. *Bull. Amer. Phys. Soc*, ser. 1, **16**, 825–826, (1971).
- [5] P.J. Shlichta. Higher dimensional Hadamard matrices. *IEEE Trans. Inform. Theory*, **IT-25**, 566–572, (1979).
- [6] Y.X. Yang. Theory and applications of higher-dimensional Hadamard matrices. Combinatorics and Computer Science Series. Beijing: Science Press. Dordrecht: Kluwer Academic Publishers, (2001).

# $A_\infty$ -Persistence

Francisco Belchí Guillamón (Kiko), Aniceto Murillo Mas  
University of Málaga (Spain)

frbegu@gmail.com

## Abstract

Classical persistence [1], in very general terms, gives the observer a good presentation of data related with the homology of a (time or other parameters dependent) complex which usually arises from some applied setting (digital images, sensor networks, data analysis,...). However, any (co)homology theory can be endowed with extra algebraic structures which may also reveal some special behaviour of the considered situation.

Thus, inspired by computational approaches to  $A_\infty$ -structures by Pedro Real et al. through Discrete Morse Theory and the Homotopy Perturbation Lemma [2], we develop a theory of persistence for  $A_\infty$ -structures on (co)homology, with the hope of filtering in a finer way the noise arising in 3D digital images.

## References

- [1] H. Edelsbrunner and J. Harer, Computational topology: An introduction, Applied mathematics, American Mathematical Society, 2010.
- [2] A. Berciano, H. Molina-Abril, P. Real. Searching high order invariants in computer imagery. *Applicable Algebra in Engineering, Communications and Computing*, v.23 (Issue 1-2) pp. 17-28, 2012

Partially supported by Ministerio de Educación y Ciencia, project MTM2010-18089.

# Discrete Morse theory and computational homology.

Paweł Dłotko  
University of Pennsylvania  
dlotko@sas.upenn.edu

## Abstract

During the last 15 years some classical concepts from pure mathematics have become computationally tractable. Also a few other concepts have been discovered until that time. The classical concepts which are now routinely computable are homology and cohomology groups and their generators. The new concepts, which were introduced along with algorithms to compute them, are standard and zigzag persistence.

At the same time, somehow independently discrete Morse theory and its computational methods has been developed. They have been used to simplify functions on surfaces, denoising, and in some situation to obtain Betti numbers.

Still, both computational homology and discrete Morse theory provide information about evolution of level sets of some function defined on a cell complex. In this talk we will show how, using discrete Morse theory, one can obtain information about field homology, persistence and zigzag persistence. Consequently, we will show, that discrete Morse theory is a main branch from which all the described computational methods can be derived.

This talk is based on joint work with Vidit Nanda and Hubert Wagner.

## Keywords

Discrete Morse theory, computational homology, persistence, zigzag persistence, computations

# Some advances in $G$ -invariant persistent topology and homology

Patrizio Frosini  
University of Bologna (Italy)

patrizio.frosini@unibo.it

## Abstract

It is well known that classical persistent homology is invariant under the action of the group  $\text{Homeo}(X)$  of all self-homeomorphisms of a topological space  $X$ . As a consequence, this theory is not able to distinguish two filtering functions  $\varphi, \psi : X \rightarrow \mathbb{R}$  if a homeomorphism  $h : X \rightarrow X$  exists, such that  $\psi = \varphi \circ h$ . This fact greatly restricts the use of classical persistent homology in shape comparison. As a trivial example, we can think of a gray-level image represented by a function  $\varphi : \mathbb{R}^2 \rightarrow \mathbb{R}$ . Obviously, the substitution of  $\varphi$  with  $\varphi \circ h$  can greatly change the appearance of the image, for  $h \in \text{Homeo}(\mathbb{R}^2)$ . The following question naturally arises: How can we adapt the concept of persistence in order to get invariance just under the action of a proper subgroup of  $\text{Homeo}(X)$  rather than under the action of the whole group  $\text{Homeo}(X)$ ?

In this talk we will illustrate how this problem can be managed by means of  $G$ -invariant persistent homology [1] and other recently developed techniques.

## Keywords

Size function, persistent homology, natural pseudo-distance

## References

- [1] P. Frosini, *G-invariant Persistent Homology*, AMS Acta, Università di Bologna, 3614 (2012). Preprint. Available also at [arXiv:1212.0655](https://arxiv.org/abs/1212.0655).

# Boundary and acyclicity operators of primal and dual elementary cell complexes\*

Ana Pacheco, Pedro Real  
University of Seville (Spain)  
ampm@us.es

## Abstract

In this paper, we compute the boundary and acyclicity algebraic operators of each of the 23 elementary cell complexes in the context of the discrete combinatorial geometry developed by Kenmochi and Imiya [1]. Moreover, we compute the boundary and acyclicity operators of the barycentric dual cell complex of each of these elementary cell complexes. Finally, we present some conclusions about the relationship between the boundary and acyclicity algebraic of an elementary cell complex and its corresponding dual cell complex.

## Keywords

discrete combinatorial geometry, cell complex, dual cell complex, algebraic topology, homology

- [1] Y. Kenmochi and A. Imiya. Combinatorial boundary of a 3D lattice point set. *Visual Communication and Image Representation* 17(4): 738–766, 2006.

---

\*Partially supported by Ministerio of Educación y Ciencias and FEDER funds project 4D-Hom:MTM2009-12716

# A chain contraction approach to the computation of cubical homology and cohomology\*

Paweł Pilarczyk  
University of Minho (Portugal)

Pedro Real  
University of Seville (Spain)

<http://www.pawelpilarczyk.com/>

## Abstract

Algorithms for the computation of homology, cohomology, and related operations on cubical cell complexes are introduced, using the construction of a chain contraction from the original chain complex to a reduced one that represents its homology. As opposed to the “traditional” approach in which the Smith Normal Form of boundary matrices is computed, the additional structure provides considerably more comprehensive homological information. With this technique, one can instantly determine the homology class of any cycle, which allows computing (co)homological operations (like the cup product in cohomology) much more easily than in the approach in which the SNF alone is computed. This work is based on previous results for simplicial complexes obtained by Pedro Real, Roxio Gonzalez-Diaz, and their collaborators, and uses Serre’s diagonalization for cubical cells.

## Keywords

Algorithm, Software, Homology, Cohomology, Computational homology, Cup product, Alexander-Whitney coproduct, Chain homotopy, Chain contraction, Cubical complex, Cubical homology

---

\*This research was partially financed from Fundo Europeu de Desenvolvimento Regional (FEDER) through COMPETE – Programa Operacional Factores de Competitividade (POFC) and from the Portuguese national funds through Fundação para a Ciência e a Tecnologia (FCT) in the framework of the research project FCOMP-01-0124-FEDER-010645 (ref. FCT PTDC/MAT/098871/2008). P. Real was additionally supported by the Spanish Ministry of Science and Innovation, project no. MTM2009-12716.

# Computational Homological Algebra for Advanced Topological Analysis of 4D digital images

Pedro Real  
University of Seville (Spain)  
real@us.es

## Abstract

We deal with here the complex problems involved in adapting and efficiently applying algebraic topology-based methods for the analysis of digital images up to four dimensions. To achieve this, an underlying mathematical and computational framework to exploit homology-based tools (related to the notion of  $n$ -dimensional holes) in diverse 4D discrete settings is generated. The computational nature of homology information and close connection to applications is highlighted using new homological algebra notions such as chain-integral complexes and equivalences. This algebraic machinery works with two nilpotent algebraic operators acting on the same graded module. It is more than a mere extension of the classical homotopy category of chain complexes, allowing us to establish a graph-based topological representation of a subdivided object and a strong interplay between Discrete Morse Theory and Algebraic-Topological Models. Restricted to real coefficients, it also helps us in reinterpreting and exploiting homology information and in finding general harmonic representative classes.

From a theoretical point of view, the research will be focused on the following topics: Homological Modeling, Analysis and Acuity for 4D digital images. These three issues are developed using chain-integral tools.

Concerning Homological Modeling, the idea is to construct a continuous analogous of 4D digital objects (based on square hypercubes) and to develop homology and geometry computation algorithms based on the chain-integral homology (CHI) framework. 402 non-isometric hyper-polyhedra are the elementary bricks of this local-to-global topological approach [5] which aims to establish results harmoniously combining geometry and topology.

For advancing in 4D-knowledge, it is compulsory to clarify the nature and role of topology in the digital imagery setting, and to try and positively answer the related problems of robustness with respect to noise and dimensionality reduction. We develop a topological processing framework of 4D digital images, which is consistent, robust, flexible and reusable [4, 2, 3, 1]. We use global combinatorial stuff (mainly, graphs and trees) in order to do advanced topological analysis at two levels: Cocyclic calculus (topological skeletons, Reeb graphs, classification of cycles, contractibility and transformability of cycles, cocyclic operations, ...) and Homological Calculus (homology and cohomology classes, homology  $A(\infty)$ -coalgebra, cohomology ring, cohomology operations, homotopy operations,...).

## Keywords

Computational Homological Algebra, chain-integral equivalences, 4D digital image, algebraic modelling,  $\chi$ -calculus, cocyclic calculus, homology calculus, homological classification, topological skeletons, homology  $A(\infty)$ -coalgebra, homotopy groups

## References

- [1] A. Berciano, H. Molina-Abril, P. Real. Searching high order invariants in computer imagery. *Applicable Algebra in Engineering, Communications and Computing*, v.23 (Issue 1-2) pp. 17-28, 2012 DOI: 10.1007/s00200-012-0169-5
- [2] H. Molina-Abril, P. Real. Homological Optimality in Discrete Morse Theory through chain homotopies. *Pattern Recognition Letters* (ISSN: 01678655), v. 33 (Issue 11), pp. 1501-1506, 2012. DOI: 10.1016/j.patrec.2012.01.014
- [3] H. Molina-Abril, P. Real. Homological spanning forest framework for 2D image analysis. *Annals of Mathematics and Artificial Intelligence*, v. 64 (Issue 4) pp. 385-409, 2012. DOI: 10.1007/s10472-012-9297-7

[4] Helena Molina Abril Homological Spanning Forest for Discrete Objects. Universidad de Sevilla. Advisor: prof. P. Real (Univ Sevilla). Dpto de Matemática Aplicada I (ETS Ingeniería Informática) July, 2012

[5] Ana Mara Pacheco. Extracting cell complexes for 4-dimensional digital images. Advisors: prof. Pascal Lienhardt (Universit de Poitiers, France) and prof. P. Real (Universidad de Sevilla). Universidad de Sevilla, Dpto de Matemática Aplicada I (ETS Ingeniería Informática) July, 2012

*Partially supported by Ministerio of Educacin y Ciencias and FEDER funds project 4D-Hom:MTM2009-12716*

[



# Spectral sequences for computing persistent homology of digital images\*

Ana Romero, Gadea Mata, Julio Rubio  
University of La Rioja (Spain)

Jónathan Heras  
University of Dundee (UK)

Francis Sergeraert  
University Joseph Fourier (France)

`ana.romero@unirioja.es`

(See short paper in Appendix, pag. 331–335)

## Abstract

Persistent homology [1] is an algebraic method for measuring topological features of shapes and functions, which can be applied to study digital images. More concretely, this technique consists in identifying homological features that persist within the different stages of a filtration. On the other hand, spectral sequences [2] are a tool for computing homology groups by taking successive approximations. Both concepts are deeply related.

In a previous work [3], we showed that a slight modification of our previous programs for computing spectral sequences [4] is enough to compute also persistent homology. By inheritance from our spectral sequence program, we obtained for free persistent homology programs applicable to spaces not of finite type (provided they are spaces with effective homology) and with  $\mathbb{Z}$  coefficients (significantly generalizing the usual presentation of persistent homology over a field).

In this work, we will use our programs in order to compute persistent homology of digital images, which will allow us to determine relevant features, that will be long-lived – in the sense that they persist over a certain parameter range – on contrast with the “noise” which will be short-lived. As a test case, our programs could be applied on a fingerprint database.

## Keywords

Persistent homology, digital images, spectral sequences.

## References

- [1] H. Edelsbrunner and J. Harer, *Computational topology: An introduction*, Applied mathematics, American Mathematical Society, 2010.
- [2] S. MacLane, *Homology*, vol. 114, Springer, 1963.
- [3] A. Romero, J. Heras, J. Rubio, and F. Sergeraert, *Defining and computing persistent  $\mathbb{Z}$ -homology in the general case*, Preprint, 2013.
- [4] A. Romero, J. Rubio, and F. Sergeraert, *Computing spectral sequences*, Journal of Symbolic Computation **41** (2006), no. 10, 1059–1079.

---

\*Partially supported by Ministerio de Educación y Ciencia, project MTM2009-13842-C02-01.



---

# Session 11: Symbolic and Numerical Methods: Practical Applications

---

**Organizers:**

**José Manuel González Vida  
Tomás Morales de Luna  
María Luz Muñoz Ruiz**



# A numerical and an exact approaches for classifying the items of a questionnaire into different competences

José Luis Galán, Salvador Merino, Javier Martínez, Miguel de Aguilera  
University of Málaga (Spain)

jl\_galan@uma.es

## Abstract

In ([1]) a Likert scale is defined to be a psychometric response scale primarily used in questionnaires to obtain participant's preferences or degree of agreement with a statement or set of statements. Respondents are asked to indicate their level of agreement with a given statement by way of an ordinal scale. The most commonly used is a 5-point scale ranging from "Strongly Disagree" on one end to "Strongly Agree" on the other with "Neither Agree nor Disagree" in the middle.

Normally, when a company wants to check the capabilities and skills of their employees (or when looking for new employees), a huge Likert scale questionnaire is asked to be filled up. With such a questionnaire, different competences are evaluated and therefore, the result of a questionnaire will provide important information about capabilities and skills of the respondents for each competence.

As an example, we will describe, for a real questionnaire of 170 Likert items (questions) and 23 competences, how to classify each question with the corresponding competence. That is, to find out, for each Likert item, which competence is evaluated. We will present how to face and solve the problem using two different techniques:

1. **A numerical approach**, using the theory of genetic algorithms.

John Henry Holland is considered the father of Genetic Algorithm by adapting Charles Darwin's natural selection theory to Artificial Intelligence.

In the computer science field of artificial intelligence, a genetic algorithm is a search heuristic that mimics the process of natural evolution ([2]). This heuristic is routinely used to generate useful solutions to optimization and search problems.

Genetic algorithms belong to the larger class of Evolutionary Algorithms, which generate solutions to optimization problems using techniques inspired by natural evolution, such as selection, genetic engineering, crossover, mutation and cloning.

These concepts will be adapted to the example and later we will describe the solution found. This technique required software which deals with numeric approximations (specifically, we used MATLAB).

One of the main advantages of this method is that this numerical approach can even be used when there are less equations (filled questionnaires) than unknowns (items) and this technique can lead to find the required solution.

2. **An exact method**, by solving a quadratic system of  $n$  equations and  $n$  unknowns.

We will show how this quadratic system was built and how it can be converted to a linear system which provides the solution in a easy way. This technique required the use of a Computer Algebra System (specifically, we used DERIVE) for exact computations.

One of the main advantages of this technique is that if there are enough equations, this exact method will lead to the solution faster than the numerical approach.

After this example, we will set the basics to solve this competence-assignment problem for a generalized version of similar questionnaires with  $n$  Likert items for evaluating  $m$  competences using both techniques.

Both techniques were first introduced and presented in the "Nonstandard Applications of Computer Algebra" Special Session at ACA 2012 ([3]). In this case, we present improved versions of both techniques which can be used even when there exists some errors in the data.

Also, we will show the results obtained when applying this new improved versions to another example of a huger Likert questionnaire.

Finally, we will describe also other advantages and disadvantages of both techniques in addition of the ones described above.

### **Keywords**

Likert's questionnaires, competences, genetic algorithms, Numerical Methods, CAS

## **References**

- [1] Likert Scale, Wikipedia. [http://en.wikipedia.org/wiki/Likert\\_Scale](http://en.wikipedia.org/wiki/Likert_Scale)
- [2] Genetic Algorithm, Wikipedia. [http://en.wikipedia.org/wiki/Genetic\\_algorithm](http://en.wikipedia.org/wiki/Genetic_algorithm)
- [3] J. L. Galán, S. Merino, J. Martínez, M. de Aguilera. Classifying the items of a Likert based questionnaire in different competences. Applications of Computer Algebra Conference, ACA 2012, <http://math.unm.edu/~aca/ACA/2012/Nonstandard/Galan.pdf>.

# Optimization and design of bicycles lines

Roberto José Liñán Ruiz  
University of Córdoba (Spain)

Salvador Merino Córdoba, Javier Martínez Del Castillo  
University of Málaga (Spain)

roberto.j.l.ruiz@gmail.com, smerino@uma.es, jmartinezd@uma.es

## Abstract

The approach to urban planning has started to change in recent years over many cities. What used to be privileges for motor vehicles, are now incentives to the development of sustainable transport modes among which cycling lanes play a substantial role.

With the development and construction of this kind of facilities, there has been an insufficient coordination between different modes of transportation. This has been due mainly to the lack of comprehensive studies, which have caused the expected intermodality to fail.

By applying graph theory, mathematical models were developed, calculations were made, and optimized designs were achieved for this kind of infrastructure. These results make it possible to use resources more efficiently and to improve cycling paths that already exist.

These calculations were performed using the computer algebra tool under symbolic computation SAGE. In this article we present the graph methods used for optimization along with the final design of bicycle lanes that were obtained.

## Keywords

Optimization, Routes, Algorithm, SAGE

## 1 Introduction

Over recent years, the evolution, transformation and development of the urban fabric of cities and their surroundings has occurred at a rapid pace. These changes have had a primary purpose: mobility.

The economic impact makes urban infrastructure costs to maintain mobility model based on the predominant use of the car pose a significant economic cost in the design, implementation and maintenance of new infrastructure oriented at that.

It has begun to consider taking necessary steps to managing mobility demand by diversifying and promoting less aggressive modes and consume less floor and resources: the walking, public transport and bicycle. Currently, each of the administrations has been dedicated to developing mobility plans to promote, facilitate and incorporate the bicycle as a means of transportation optimal.[For94]

Therefore, it is necessary to discuss new standards in sustainable mobility to address the problems of increasing car use as a basis for the design of tools for planning and management more effective. Is necessary a planning to promote sustainable mobility model that produces a city transport efficient less and private vehicle use and more conducive to the use of urban transport and, in particular, the bicycle transportation.[O&97]

The development and evolution of geographic information systems (GIS) has facilitated their use in urban planning and organization of the city and territory. This, coupled with the use of mathematical systems as graph theory, allows a study, design and calculation of future transport networks.

In this particular case, the use of graph theory allows guarantees ensure that spending on the design and construction of networks for bicycle is better planned with predictions based on data from studies mathematically, from graph theory, as it seeks to develop this algorithm.

The development of the algorithm that is developed, objectively, tidy and actual functionality, the optimal design from the using of graph theory, as is being done in the different modes of

transport studies, provides a new way responsible, orderly and economic of infrastructure design for the use of bicycles.[Li12]

## 2 Approach of problem

Currently, there are various studies that present examples of optimization of public transport routes. For this type of route is important to consider the distances to travel, since this will depend on travel time, the cost thereof, the improvement of the service and, above all, most importantly, customer satisfaction.

For the calculation of such routes, the software uses as a starting point Dijkstra's algorithm, also called shortest path algorithm. An algorithm for determining the shortest path given a source point to other points in a directed graph with weights (distances) on each edge.

Within the study from graph theory, is implemented Dijkstra algorithm through the computer system and thus provide a more practical solution to the problem of optimal design of bicycles lanes.

This new algorithm created part of using the minimum distance calculation for public transport, but to apply it to the calculation and design to develop new bicycle lanes.

The idea behind this new algorithm created is to go exploring all shortest paths that start from the origin point and lead to all other points, when you get the shortest path from the source point, the rest of vertices that make up the graph, but incorporating a number of variables that complement the algorithm to achieve a solution that not only depend on the shortest path, so depend the analysis of all the variables that are formulated in this new algorithm.

As immediate goal is to get the best route planning or appropriate design for the network, for use with bicycles. This algorithm is an improved algorithm for computing minimal paths in graphs. There are two important parts to note:

1. The objective function: the primary goal is to minimize "costs". In this case, cost is considered as the sum of all variables that are taken into consideration in the calculation of the networks.
  - (a) Shortest Path.
  - (b) Minimum Time.
2. Restrictions: For a complete study, design and planning of networks must meet certain variables or constraints.
  - (a) Social / Political.
  - (b) Types of Streets.
  - (c) Slope.
  - (d) Etc.

Shortest path calculation is applied in graph theory is based on obtaining the fastest route or shorter, depending on the variables to study, these variables are often time or distance, respectively.

Achieving of new algorithm ensures that this mathematical system that is created meets an unmet need at present to design and plan the routes for the infrastructure for the use of bicycles, increasing of study variables. These variables are the restrictions or the end condition the good design of future cycling infrastructure.

## 3 Algorithm design

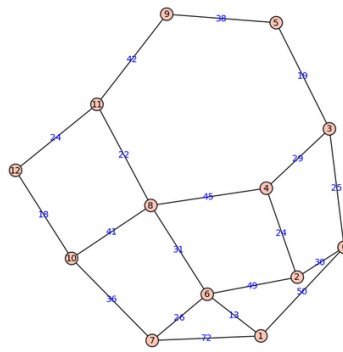
As previously mentioned, this new algorithm is based on graph theory algorithms that are able to calculate the shortest paths within any graph.

A graph is defined by its matrix structure incidence and adjacency matrix. From its adjacency matrix, calculated the matrix with weights previously established in a database.

### **Length:**

The first variable to consider is that of length. For route calculation is considered more important. Once you have the graph with all weights on its edges, in this case is the length, we proceed to calculate the matrix with mathematical program like Sage and drawing the graph with her weights.





For this variable, the minimum distance calculation is straightforward, so once you get the graph with their weights, we proceed to calculate the shortest path between point 0 and 12.

```
g.shortest_path_all_pairs()
g.shortest_path(0, 12, by_weight=True)
[0, 1, 6, 8, 11, 12]
```

**New Variables:**

To calculate a minimum path efficiently is necessary to incorporate new variables, not just the length, there has been a series of calculations to relate each of the new variables to the initial study.

$$MATRIX(A) \times \delta_A + MATRIX(A) \times \sum [MATRIX(B) \times \delta_B \times \beta_B] + \dots + [MATRIX(N) \times \delta_N \times \beta_N]$$

Where:

$\delta_N$  = % of importance given to variables.

$\beta_N$  = variables coefficients.

$\beta_A$  = slope's coefficients. =  $(1 + \frac{\gamma_B}{100})$

$\beta_B$  = traffic light's coefficients. =  $(1 + \frac{\gamma_C}{100})$

$\beta_C$  = social-political's coefficients. =  $(1 + \frac{\gamma_D}{50})$

\* For these examples has been given equal importance to the variables, so has the same value.

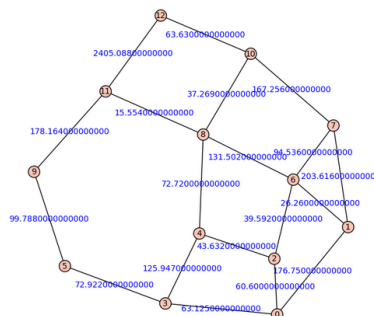
**A) Slope.**

One of the main variables to be taken into account in calculating optimal routes is the slope. The start of this variable is similar to the lengths, first calculate its matrix and graph with weights with Sage. Once is obtained the slopes matrix, must be multiplied by the coefficient variable length to relate.

$$MATRIX(B) \times \delta_B \times \beta_B$$

This achieves the matrix which affects the lengths. This matrix highlights how much can harm or surpass the lengths of the sections, for that this matrix is calculated with the matrix given lengths, but point to point in each array.

Once calculated this new matrix, you draw your graph with their respective new weights.



Now we just calculate the minimum distance for the length and the slopes of the sections together.

```

g.shortest_path_all_pairs()
g.shortest_path(0, 12, by_weight=True)
[0, 2, 4, 8, 10, 12]

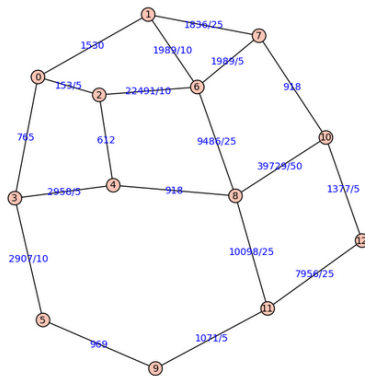
```

**B) Traffic lights.**

This section includes the time of the traffic lights in the area to be studied. For this case an average calculation of the time of the red lights and the likelihood of meeting them in the same color. Once you have given the values for each of the streets, is necessary to calculated Matrix and Graph with corresponding weights. AFter to obtain the traffic lights matrix, must be multiplied by the coefficient variable length to relate.

$$MATRIX(C) \times \delta_C \times \beta_C$$

This ensures the traffic lights matrix on the lengths. This matrix highlights how much can harm or surpass the lengths of the sections, for that this matrix is calculated with the matrix given lengths, but point to point in each array. Once calculated this new matrix, you draw your graph with their respective new weights.



Now we just calculate the minimum distance for the length and the traffic light of the sections together.

```

g.shortest_path_all_pairs()
g.shortest_path(0, 12, by_weight=True)
[0, 2, 4, 8, 11, 12]

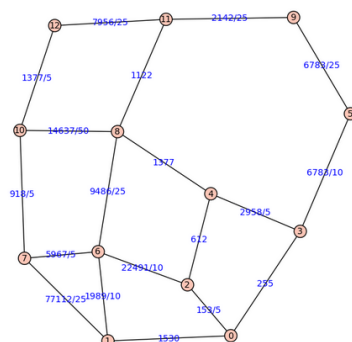
```

**C) Social-Political.**

This value is assigned by the importance that can be attributed to some streets in the city, due to the existence of schools, or any type of infrastructure that is priority when building or designing a bike path near it. Once you have given the values for each of the streets, is necessary to calculate the Matrix and Graph with corresponding weights. After to obtain the social/politicals matrix, must be multiplied by the coefficient variable length to relate.

$$MATRIX(D) \times \delta_D \times \beta_D$$

This ensures the social-politicals matrix on the lengths. This matrix highlights how much can harm or surpass the lengths of the sections, for that this matrix is calculated with the matrix given lengths, but point to point in each array. Once calculated this new matrix, you draw your graph with their respective new weights.



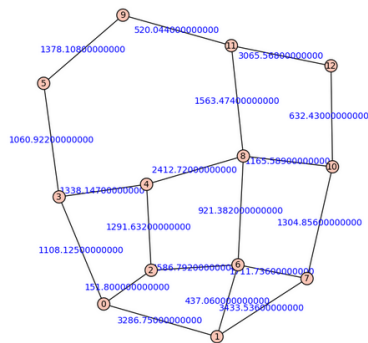
Now we just calculate the minimum distance for the length and the social-political of the sections together.

```
g.shortest_path_all_pairs()
g.shortest_path(0, 12, by_weight=True)
[0, 3, 5, 9, 11, 12]
```

## 4 Algorithm's checking

After to calculate each of the variables, it proceeds to the testing and demonstration of the algorithm. This shall be the sum of the final matrices calculated for each of the cases.

$$MATRIX(A)+MATRIX(A) \times \sum [MATRIX(B) \times \beta_B] + [MATRIX(C) \times \beta_C] + [MATRIX(D) \times \beta_D]$$



Once calculated the Final Graph with weights of all variables that have been studied for this case (Lenght, Earrings, Traffic Light and Social-Politician) should calculate the minimum distance to verify the functionality of the new algorithm.

```
g.shortest_path_all_pairs()
g.shortest_path(0, 12, by_weight=True)
[0, 2, 4, 8, 10, 12]
```

As can be seen, the Shortest Path to travel from point 0 to 12 has been changed with the calculation of the different variables that have been studied. This indicates that the algorithm is feasible for the calculation and design of this case.

In essential for the use of this algorithm is to have the database to be appropriate for each of the cases studied. After obtaining each of these variables, we can design optimal routes for this type of infrastructure, allowing a great improvement in the future construction of cycle lanes, encouraging the use of citizens of these infrastructures and improving the sustainable transport in cities.

## References

[For94] J. Forester. *Bicycle transportation: a handbook for cycling transportation engineers*. Mit Press, 1994.

[Li12] R. J. Lian. *EStudio y optimizacin del carril bici de Mlaga*. Trabajo Fin de Master. Universidad de Mlaga, 2012.

[O&97] C.A. O&Flaherty. *Transport Planning and Traffic Engineering*. Engineering village. Arnold, 1997.

# Resolution of solar cells equivalent electrical model by reverse decomposition

Salvador Merino & Francisco J. Sánchez & Pedro Rodríguez & Carlos Sánchez  
University of Málaga (Spain)

smerino@uma.es , fsanchezp@uma.es  
prodriguez@uma.es , csanchez@malaga.eu

## Abstract

It is broadly extended that the electrical equivalent model equation of a solar cell is developed where its variables are solved in an implicitly way. The resolution of these equations allows us to properly estimate the operating voltage of the different solar cells and hereupon we can predict the electricity generated.

In this equation, some variables are affected of ambient conditions (solar radiation level, ambient temperature, etc.). Additionally, some correction factors must be applied so that to subtly modify the previous calculation and approximate the theoretical model to final yield found.

To solve these equations we have proceeded, following the philosophy of predictor-corrector methods well-known as Adam-Bashforth and Adam-Moulton, to develop a methodology that we have named as "reverse decomposition". Having demonstrated the initial conditions to be met by the decomposition made, we proceeded to apply them on electrical behavior equations. The methodology has been developed under CAS systems (Computer Algebra System), and programmed with wxMaxima software.

## Keywords

numerical methods, sustainability, solar energy, wxMaxima

# Using CUDA for better harnessing of symbolic and numerical methods

S. Ortega Acosta<sup>1</sup>, J.M. González Vida<sup>1</sup>, T. Morales de Luna<sup>2</sup>,  
M.L. Muñoz Ruiz<sup>1</sup>, C. Sánchez Linares<sup>1</sup> .

<sup>1</sup> University of Málaga (Spain)

<sup>2</sup> University of Córdoba (Spain)

`sergio.ortega@uma.es`

## Abstract

CUDA (Compute Unified Device Architecture) is a parallel computing platform and programming model created by Nvidia and implemented for the graphics processing units (GPUs). A wide range of functions of symbolic and numerical mathematical software can be enhanced using CUDA, delivering dramatic performance gains. Areas as image processing, linear algebra, financial simulation, Fourier transforms, etc. can be GPU-enhanced. In this talk we will show how a CUDA-framework can be implemented in order to improve desktop mathematical software as Wolfram Mathematica or Matlab and online mathematical software as Sage.

## Keywords

CUDA, Graphic Processor Units, enhanced symbolic and numerical software

# Numerical algorithm solves for a new positioning system inside buildings

Ana Belén Pabón  
University of Córdoba (Spain)

Salvador Merino  
University of Málaga (Spain)

Pedro Rodríguez  
University of Málaga (Spain)

`ig2padua@uco.es`

## **Abstract**

We present numerical algorithm solves for a new positioning system using techno-accessibility inside buildings, whose platform is Power line communication (PLC).

This system has been implemented using computer algebra programmes, in order to properly locate the user in a spot inside the building with this new technology. For this we proceeded to calculate their position coordinates taking into account: signal travel time, the wave speed, the interference due to changes in temperature and density through the means which it travels.

In the system there are associated several existing methods and infrastructures: electricity network, internet, web pages, Wi-Fi, GNU General Public License, Bluetooth, Radio Frequency Identification, computers and servers.

The end user will be guided through a smartphone using images and/or voice and will allow you to know the possibilities offered by the facilities where you are situated.

The data is processed under wxMasima and can have a wide variety of functions such as: creating virtual 3Dmodels of building, situation within them and added services. All this is the key to user- level interaction.

After its development and implementation, the horizon of this future is exciting. Its range will cover a vast diversity of applications and provide a variety of uses, as takes place with current GPS navigations system outdoors. Some of these new applications will be present as the culmination of this work.

## **Keywords**

Techno-accessibility, PLC, Indoor navigation, Numerical algorithm solves, 3Dmodels, Smartphone, Intelligent building, Positioning system, Apps

# Kinematical analysis of mechanisms with computer algebra

Samuli Piipponen, Teijo Arponen, Jukka Tuomela  
University of Eastern Finland, Department of Physics and Mathematics

samuli.piipponen@uef.fi

## Abstract

Mechanisms appearing in engineering sciences are devices which are usually composed of different types of rigid bodies which are put together with different types of joints. The joints connecting the bodies impose different types of *constraint equations* between the coordinates of the bodies. If the mechanism consists of open kinematical loops the analysis of its configuration space is typically rather straightforward, but in the presense of closed loops the analysis is usually a lot more complicated.

From mathematical point of view the kinematical analysis is simply the analysis of the solution set imposed by the constraint equations. In many cases the solution set can be treated as an *algebraic variety* defined by the constraints. In engineering terms this is referred to as the *configuration space* of the mechanism. This allows us to use the state of the art computational methods and Gröbner bases techniques in the actual algebraic analysis of the *constraint ideal* generated by algebraic constraint equations.

Most interesting questions from engineering point of view are the *mobility* (degrees of freedom, dof) and various *singularities* (for example changes in mobility) of the configuration space. In our context the mobility is simply the dimension of the corresponding variety and singularities are singularities of this variety.

In many cases the configuration space can have components of different dimension. As an algebraic variety the configuration space has natural *irreducible decomposition* which corresponds to the *prime decomposition* of the constraint ideal. The connected components of different irreducible components are called *motion modes* of the system and the maximal connected unions of these components are called *assembly modes* of the mechanism.

We will show, using several nontrivial examples, how we can effectively use computer algebra and Gröbner bases techniques to study the mobility and singularities of given systems. Moreover we will demonstrate how we can simplify the actual constraints to enhance the dynamical analysis of the mechanisms.

## Keywords

Kinematical analysis, Computer algebra, Gröbner bases, Ideal decompositions

# CAS software for teaching numerical methods in engineering. Practical applications

C. Sánchez Linares<sup>1</sup>, J.M. González Vida<sup>1</sup>, T. Morales de Luna<sup>2</sup>,  
M.L. Muñoz Ruiz<sup>1</sup>, S. Ortega Acosta<sup>1</sup>.

<sup>1</sup> University of Málaga (Spain)

<sup>2</sup> University of Córdoba (Spain)

`csl@uma.es`

## **Abstract**

The objective of this talk is to present different applications of CAS software to solve practical problems in engineering. This practical applications will be the departing point for teaching numerical methods in engineering. CAS software has the advantage of allowing students to confront real life examples in an easy way. Moreover, resolution of such problems will motivate and justify numerical methods in engineering.

As a particular case we will show some examples using Sage and SymPy which are Open Source.

## **Keywords**

CAS, Symbolic mathematics, Sage, SymPy



# Statistical Quality Control in the Construction Industry

José Antonio Vera López  
University of Córdoba (Spain)

Salvador Merino Córdoba, José Luis Galán García  
University of Málaga (Spain)

`javl.istan@hotmail.com`, `smerino@uma.es`, `jl.galan@uma.es`

## Abstract

Algebra applications for computers are an essential tool for solving complex problems. Among the variety of programs that exist nowadays, in this paper we will choose wxMaxima as open source computer algebra system for symbolic computation on Lisp language.

This software will be applied to the statistical control of quality, which is commonplace in many business areas and most developed in mass production industries. Authors such as Juran, Deming and Ishikawa have contributed substantially to this field.

In the case of construction industry, quality control is often carried out very poorly. Minimum legal requirements are usually the target, causing serious trouble to the works and adding unexpected costs.

For this reason, this article aims to transfer quality control statistical methods that have been successful producing industry-scale objects, to an industry which is quite distant to it, such as construction. Algorithmic development under wxMaxima was used in order to solve and implement this approach.

## Keywords

Statistical methods, Quality Control, Construction, wxMaxima

## 1 Introduction

Quality control in the construction industry is becoming increasingly necessary. The speculation and the mass production of the works make the quality is careless. The requirement of a quality control should be developed as a general rule. Its to avoid (prevent) not only the customer dissatisfaction, but risks and losses due to little or no quality control in the construction.

The statistical control is one of the solutions to this problem. It was Born in the late 20's at Bell Laboratories. Its inventor was A. Shewhart, who in his book "Economic Control of Quality of Manufactured Products" [She31](1931) set the standard that would follow other distinguished disciples (J. Juran, W.E. Deming, K. Ishikawa).

The statistical control is based on the variations that are produced when a production process is executed in normal conditions. The results that are obtained to examine the products made in the process tend, generally, to a Gaussian distribution. In which it is seen that half of the results will be below an average value and half above.

The causes of variations can be:

- **Random causes:** They are inherent to the process, which appear and disappear of random form, producing a regular variability that can be reduced but not removed.
- **Assignable causes:** They are caused by specific reasons.

A process is under statistical control when only random causes act. The variation of the results it will be found in the range given by:

$$\mu \pm \varepsilon_m \dots (1)$$

Where:

$\mu$  is process mean.

$\varepsilon_m$  is inherent error of the production process, given by the equation:

$$\varepsilon_m = \frac{t\sigma}{\sqrt{n}} \dots (2)$$

In which:

$t$  is factor that depends of the level of confidence.

$\sigma$  is standard deviation of the process.

$n$  is sample size.

Where in a specific production process act one or more assignable causes, is said that the process is out of statistical control. As there is a high probability that the variations are outside the range described above. It's being necessary to identify the causes that produced them. With the purpose of remove at the appropriate time to avoid the nonconformity, the waste of time and the increased cost.[JGB83]

Statistical analysis of the results which are obtained from the measurements and testing in all phases of a specific production process, allow to conclude if the process is in statistical control or early detection the occurrence of assignable causes that put out of statistical control. It's can be performed through control charts.

## 2 Control Charts

One of the techniques which it is applied in statistical control is control charts. They analyze the evolution over time of a quality characteristic of which variation is wanted to control (ordinate axis), based on the controlled product units (abscissas axis).

In the control chart is recorded the different values of the characteristic. If are joined the different values, it is obtained a broken profile, called graph trends. The control chart is completed by the statistical control limits. They are three horizontal lines that are identified with the values defined of the characteristic to control, that are interesting to valuate the process stability: Lower Statistic Limit, Central Statistic Limit or Average Quality and Upper Statistical Limit. These limits should not be confused with specification limits and optimal central value, which are technical and have a different meaning.

The characteristics submitted to control in a graph can be of two types: attributes and variables. The attributes are characteristics that can only take a limited number of values, one or two. Their presence in the product is usually indicative of a unsatisfactory quality level. The variables are continuous characteristics, can take an indeterminate number of different values, and unlike the attributes to know if it is reflected an appropriate level of quality in the product is necessary to evaluate its magnitude by a measurement process.

It exist several types of control charts. Depending on the characteristic that is analyze), it is used one or another. Although there are various methods, will be analyzed the chart of mean-standard deviation. For more information about the wide variety of control charts I recommend reading "Quality Control" of D. H. Besterfield [Bes09], where you can delve.

### 2.1 Control Chart Mean-Standard Deviation

The variables control charts are used in continuous characteristics, the determination of the value involves in performing measurements. The charts of mean - standard deviation indicate how to progress the sample mean in relation to the process mean.

In the mean chart, every time that a sample is taken, is calculated the mean value of the characteristic (3) in the observations of the sample and is represented in the chart.

$$\bar{X} = \frac{\sum_{i=1}^n X_i}{n} \dots \dots (3)$$

Where:

$\bar{X}$  is sample mean.

$X_i$  is characteristic to control of the element  $i$  the sample.

$n$  is sample size.

The average quality is corresponded with the mean of process. If process mean is not known (4), it can be used as estimate the average of the sample mean (5).

$$CL_{ST} = \mu \approx \bar{\bar{X}} \dots (4)$$

$$\bar{\bar{X}} = \frac{\sum_{j=1}^N \bar{X}_j}{N} \dots (5)$$

Where:

$\bar{\bar{X}}$  is Arithmetic average of the means of the characteristic to control for all samples.

$\bar{X}_j$  is mean of the characteristic to control of the sample j.

$N$  is sample size analyzed.

Statistical limits are calculated by the next expressions:

$$LL_{ST} = \mu + \frac{t\sigma}{\sqrt{n}} \dots (6)$$

$$UL_{ST} = \mu - \frac{t\sigma}{\sqrt{n}} \dots (7)$$

When the standard deviation of the process is unknown. It is can estimate the following way:

$$\sigma = \frac{\bar{S}}{C_4} \dots (8)$$

$$\bar{S} = \frac{\sum_{j=1}^N S_j}{N} \dots (9)$$

$$S = \sqrt{\frac{\sum_{i=1}^n (X_i - \bar{X})^2}{n - 1}} \dots (10)$$

Where:

$\bar{S}$  is the arithmetic average of standard deviation of the feature to control in all samples analyzed.

$C_4$  is a parameter experimentally determined, that implicate the standard deviation of the population and the average of the standard deviation of samples.

$S_j$  is standard deviation of the feature to control of sample j.

$S$  is standard deviation of sample.

### 3 Case study

Let us suppose that is constructed the hydraulic base of a road, for which the project specifies a degree of compaction of 95% of the maximum dry volumetric mass by AASHTO test modified, with a tolerance of 3%, and the compacting of the hydraulic base is statistically controlled with a confidence level of 95% , taking samples in steps of 250 m long and 11 wide, 5 in each.

```
(%i1) ratprint:false$
      fpprintprec:5$
      numer:true$
```

#### 3.1 Specifications

They are added the process specifications to control. They are the Specific Value (SP), the Tolerance (T) and the Acceptable Quality Level (AQL):

```
(%i4) SP:95;
```

```
(%o4) 95
```

```
(%i5) T:3;
```

```
(%o5) 3
```

```
(%i6) AQL:95;
```

```
(%o6) 95
```

### 3.2 Samples

They are added the samples obtained from each section ( $L_i$ ) analyzed.

```
(%i7) L1: [92.6,92.610,96.1,93.5,93.9];
```

```
(%o7) [92.6,92.61,96.1,93.5,93.9]
```

```
(%i8) L2: [94.5,95.1,93.2,94.7,92.4];
```

```
(%o8) [94.5,95.1,93.2,94.7,92.4]
```

```
(%i9) L3: [92.5,94.4,93.5,97,95];
```

```
(%o9) [92.5,94.4,93.5,97,95]
```

```
(%i10) L4: [97.5,92.1,97.1,93.5,93.7];
```

```
(%o10) [97.5,92.1,97.1,93.5,93.7]
```

```
(%i11) L5: [93.3,96.5,96.4,97.5,96];
```

```
(%o11) [93.3,96.5,96.4,97.5,96]
```

```
(%i12) L6: [95.7,92.4,95.2,94.7,93];
```

```
(%o12) [95.7,92.4,95.2,94.7,93]
```

### 3.3 Specific Limits

They are Calculated specification limits ( $LL_{sp}$ ,  $UL_{sp}$ ).

```
(%i13) LLsp:SP+T;
```

```
(%o13) 98
```

```
(%i14) ULsp:SP-T;
```

```
(%o14) 92
```

### 3.4 Statistical limits

They are Calculated statistical limits. The mean of the process is unknown. It is calculated as specified above (5).

```
(%i15) load(descriptive);
```

```
(%o15) C : /PROGRA/Maxima - 5.28.0 - 2/share/maxima/5.28.0 - 2/share/descriptive/descriptive.mac
```

```
(%i16) LA: [mean(L1),mean(L2),mean(L3),mean(L4),mean(L5),mean(L6)];
```

```
(%o16) [93.742,93.98,94.48,94.78,95.94,94.2]
```

```
(%i17) X:mean(LA);
```

```
(%o17) 94.52
```

The standard deviation of the process is also unknown. It is estimated as specified above (9,10).

```
(%i18) LB: [sqrt((length(L1)/(length(L1)-1))*var(L1)),  
sqrt((length(L2)/(length(L2)-1))*var(L2)),  
sqrt((length(L3)/(length(L3)-1))*var(L3)),  
sqrt((length(L4)/(length(L4)-1))*var(L4)),  
sqrt((length(L5)/(length(L5)-1))*var(L5)),  
sqrt((length(L6)/(length(L6)-1))*var(L6))];
```

```
(%o18) [1.4343,1.1345,1.6962,2.3858,1.5758,1.43]
```

```
(%i19) Y:mean(LB);
```

```
(%o19) 1.6094
```

They are required the factors  $t$  and  $C_4$

```
(%i20) load(distrib);
```

```
(%o20) C : /PROGRA/Maxima - 5.28.0 - 2/share/maxima/5.28.0 - 2/share/distrib/distrib.mac
```

```
(%i21) t:quantile_normal(1-((1-(AQL/100))/2),0,1);
```

```
(%o21) 1.96
```

```
(%i22) C4:0.94;
```

```
(%o22) 0.94
```

The statistical limits ( $LL_{st}$ ,  $UL_{st}$ ) are:

```
(%i23) LLst:X+((t*Y)/(C4*sqrt(length(L1))));
```

```
(%o23) 96.021
```

```
(%i24) ULst:X-((t*Y)/(C4*sqrt(length(L1))));
```

```
(%o24) 93.02
```

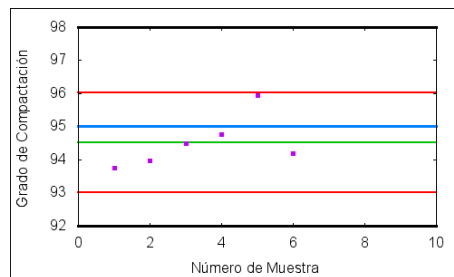
### 3.5 Control Chart Media-Standard Deviation

The control Chart Media-Standard Deviation for this process is:

```
(%i25) Puntos:makelist([i,part(LA,i)],i,1,length(LA));
```

```
(%o25) [[1, 93.742], [2, 93.98], [3, 94.48], [4, 94.78], [5, 95.94], [6, 94.2]]
```

```
(%i26) wxplot2d([ULst,LLst,X,LLsp,ULsp,SP,[discrete,Puntos]], [y,0,10],  
[style,[lines,2,2],[lines,2,2],[lines,2,3],[lines,3,5],[lines,3,5],  
[lines,3,1],[points,1,4,6]], [xlabel,"Numero de Muestra"],  
[ylabel,"Grado de Compactación"], [legend,false]);
```



## References

- [Bes09] D.H. Besterfield. *Control de calidad 8ED*. Pearson Educación, 2009.
- [JGB83] J.M. Juran, F. Gryna, and R.S.J. Bingham. *Manual del control de calidad*. Editorial Reverte, 1983.
- [She31] W.A. Shewhart. *Economic control of quality of manufactured product*. Bell Telephone Laboratories series. D. Van Nostrand Company, Inc., 1931.



---

---

## List of Participants

---

---





# List of Participants

1. Aguilera Venegas, Gabriel. Spain. `gabri@ctima.uma.es`
2. Ahmadinezhad, Hamid. Austria. `hamid.ahmadinezhad@oeaw.ac.at`
3. Alcázar, Juan Gerardo. Spain. `juange.alcazar@uah.es`
4. Alsina, Montserrat. Spain. `Montserrat.alsina@upc.edu`
5. Álvarez Solano, Víctor. Spain. `valvarez@us.es`
6. Baran, Hynek. Czech Republic. `Hynek.baran@math.slu.cz`
7. Barkatou, Moulay. France. `Moulay.barkatou@unilim.fr`
8. Bavula, Vladimir. United Kingdom. `v.bavula@sheffield.ac.uk`
9. Beaudin, Michel. Canada. `michel.beaudin@etsmtl.ca`
10. Behn, Antonio. Chile. `afbehn@gmail.com`
11. Belchí Guillamon, Francisco. Spain. `frbegu@gmail.com`
12. Botana, Francisco. Spain. `fbotana@uvigo.es`
13. Ceballos González, Manuel. Spain. `mceballos@us.es`
14. Checa, Isabel. Spain. `isabel.checa@dmat.uhu.es`
15. Cheng, Jin-San. China. `jcheng@amss.ac.cn`
16. Chèze, Guillaume. France. `guillaume.cheze@math.univ-toulouse.fr`
17. Cluzeau, Thomas. France. `cluzeau@ensil.unilim.fr`
18. Dali, Dahira. Algeria. `dddahira@gmail.com`
19. De la Villa, Agustín. Spain. `avilla@upcomillas.es`
20. Dłotko, Paweł. USA. `dlotko@sas.upenn.edu`
21. Dück, Natalia. Germany. `natalia.dueck@tuhh.de`
22. Edneral, Victor. Russia. `edneral@theory.sinp.msu.ru`
23. Escudero, Juan. Spain. `jjge@uniovi.es`
24. Falcón Ganfornina, Raúl Manuel. Spain. `rafalgan@us.es`
25. Fassino, Claudia. Italy. `fassino@dim.unige.it`
26. Ferragut, Antoni. Spain. `antoni.ferragut@upc.edu`
27. Flores Samaniego, Ángel Homero. Mexico. `ahfs@unam.mx`
28. Fortes, Inmaculada. Spain. `ifortes@ctima.uma.es`
29. Frosini, Patrizio. Italy. `patrizio.frosini@unibo.it`
30. Fúster Sabater, Amparo. Spain. `amparo@iec.csic.es`
31. Galán García, José Luis. Spain. `jl_galan@uma.es`
32. Galán García, M<sup>a</sup> Ángeles. Spain. `magalan@ctima.uma.es`
33. García López, Alfonsa. Spain. `alfonsa.garcia@eui.upm.es`
34. García Mazarío, Francisco. Spain. `gmazario@eui.upm.es`

35. Gerdt, Vladimir. Russia. `gerdt@jinr.ru`
36. Gonçalves, Tânia. Brazil. `tmng@kentforlife.net`
37. González Vida, José Manuel. Spain. `jgv@uma.es`
38. Hernando, Antonio. Spain. `ahernandoe@yahoo.com`
39. Herweyers, Guido. Belgium. `guido.herweyers@khbo.be`
40. Irtegov, Valentin. Russia. `irteg@icc.ru`
41. Jeffrey, David. Canada. `djeffrey@uwo.ca`
42. Juliá Díaz, Bruno. Spain. `bruno@ecm.ub.edu`
43. Kai, Hiroshi. Japan. `kai@cs.ehime-u.ac.jp`
44. Korporal, Anja. Austria. `anja.korporal@oeaw.ac.at`
45. Kotsireas, Ilias. Canada. `ikotsire@wlu.ca`
46. Lewis, Robert. USA. `rlewis@fordham.edu`
47. Maddah, Sumayya Suzy. France. `Sumayya-suzy.maddah@etu.unilim.fr`
48. Márquez Corbella, Irene. Spain. `imarquez@agt.uva.es`
49. Martin, Stefano. Denmark. `stefano@math.aau.dk`
50. Martín del Campo, Abraham. Austria. `abraham.mc@ist.ac.at`
51. Martínez del Castillo, Javier. Spain. `jmartinezd@uma.es`
52. Martínez Moro, Edgar. Spain. `edgar@maf.uva.es`
53. Maruri Aguilar, Hugo. United Kingdom. `H.Maruri-Aguilar@qmul.ac.uk`
54. Massarenti, Alex. Italy. `alex.massarenti@sissa.it`
55. Mencinger, Matej. Slovenia. `Matej.mencinger@um.si`
56. Merino, Salvador. Spain. `smerino@uma.es`
57. Mischczak, Jarosław. Poland. `mischczak@iitis.pl`
58. Munuera, Carlos. Spain. `cmunuera@arq.uva.es`
59. Muñoz Ruiz, María Luz. Spain. `mlmunoz@uma.es`
60. Mylläri, Aleksandr. Grenada. `amyllari@sgu.edu`
61. Mylläri, Tatiana. Grenada. `tmyllari@sgu.edu`
62. Navarro Llinares, Juan F. Spain. `Jf.navarro@ua.es`
63. Neun, Winfried. Germany. `neun@zib.de`
64. Orłowski, Arkadiusz. Poland. `arkadiusz_orlowski@sggw.pl`
65. Padilla Domínguez, Yolanda. Spain. `ypadilla@ctima.uma.es`
66. Pagani, Nicola. Germany. `npagani@math.uni-hannover.de`
67. Pečovnik-Mencinger, Andreja. Slovenia. `andreja.pecovnik@guest.arnes.si`
68. Phisanbut, Nalina. United Kingdom. `N.Phisanbut@kent.ac.uk`
69. Picard, Gilles. Canada. `gilles.picard@etsmtl.ca`
70. Piipponen, Samuli. Finland. `samuli.piipponen@uef.fi`

71. Pilarczyk, Paweł. Portugal. `pawel.pilarczyk@math.uminho.pt`
72. Pinero, Fernando. Denmark. `f.pinero@mat.dtu.dk`
73. Pletsch, Bill. USA. `bpletsch@cnm.edu`
74. Prokopenya, Alexander. Poland. `alexander_prokopenya@sggw.pl`
75. Raab, Clemens. Germany. `clemens.raab@desy.de`
76. Real Jurado, Pedro. Spain. `real@us.es`
77. Roanes Lozano, Eugenio. Spain. `eroanes@mat.ucm.es`
78. Robertz, Daniel. Germany. `daniel@momo.math.rwth-aachen.de`
79. Rodríguez, Gerardo. Spain. `gerardo@usal.es`
80. Rodríguez Cielos, Pedro. Spain. `prodriguez@uma.es`
81. Romero, Ana. Spain. `ana.romero@unirioja.es`
82. Rosenkranz, Markus. United Kingdom. `M.Rosenkranz@kent.ac.uk`
83. Rueda Pérez, Sonia Luisa. Spain. `Sonialuisa.rueda@upm.es`
84. Sáenz de Cabezón, Eduardo. Spain. `Eduardo.saenz-de-cabazon@unirioja.es`
85. Savard, Geneviève. Canada. `Genevieve.savard@etsmtl.ca`
86. Schmidt, Karsten. Germany. `kschmidt@fh-sm.de`
87. Sevilla, David. Spain. `sevillad@unex.es`
88. Shaska, Tony. USA. `shaska@oakland.edu`
89. Simón Pinero, Juan Jacobo. Spain. `jsimon@um.es`
90. Spiridonova, Margarita. Bulgaria. `mspirid@math.bas.bg`
91. Steinberg, Stanly. USA. `stanly@wendouree.org`
92. Sun, Yao. China. `sunyao@iie.ac.cn`
93. Takahashi, Tadashi. Japan. `takahasi@konan-u.ac.jp`
94. Trottier, Chantal. Canada. `Chantal.trottier@etsmtl.ca`
95. Uhler, Caroline. Austria. `caroline.uhler@ist.ac.at`
96. Ustymenko, Vasyl . Poland. `vasyl@hektor.umcs.lublin.pl`
97. Uwano, Yoshio. Japan. `uwano@fun.ac.jp`
98. Varbanoba, Elena. Bulgaria. `elvar@tu-sofia.bg`
99. Vidal, Ricardo. Spain. `rvidal@uvigo.es`
100. Villanueva, Mercè. Spain. `merce.villanueva@uab.cat`
101. Wang, Dingkang. China. `dwang@mmrc.iss.ac.cn`
102. Wester, Michael. USA. `wester@math.unm.edu`
103. Westermann, Thomas. Germany. `thomas.westermann@hs-karlsruhe.de`
104. Xue, Michael. USA. `mxue@vroomlab.com`
105. Yilmaz, Erol. Turkey. `yilmaz_e2@ibu.edu.tr`
106. Yoshida, Ruriko. USA. `Ruriko.yoshida@uky.edu`
107. Zafeirakopoulos, Zafeirakis. Austria. `zafeirakopoulos@gmail.com`
108. Zeng, Fanxuan. Spain. `fanxuan@deic.uab.cat`
109. Zeng, Peng. China. `pzeng@sei.ecnu.edu.cn`



# Authors Index

## A

Aguilera, G., 11, 15, 183, 235, 237  
Ahmadinezhad, H., 245  
Akritas, A., 11, 15, 35  
Alcázar, J. G., 163  
Algaba, A., 63  
Alsina, M., 203  
Álvarez Solano, V., 289  
Armario, J. A., 289  
Arponen, T., 311

## B

Baran, H., 83  
Barkatou, M., 11, 81  
Barrena, E., 178  
Bavula, V. V., 84  
Beaudin, M., 11, 15, 35, 43, 238  
Behn, A., 207  
Belchí, K., 290  
Bernal, J. J., 109  
Beshaj, L., 208  
Böhm, J., 11, 235  
Bonilla, J., 193  
Botana, F., 11, 161, 164  
Bruno, A., 57  
Buchberger, B., 15  
Bueno, D. H., 109  
Burlakova, L., 58

## C

Cabezas-Corcherro, J., 44  
Calmet, J., 15  
Campos, J. C., 183  
Canca, D., 178  
Cárdenas, S., 41  
Ceballos, M., 168  
Checa, I., 63  
Cheng, J. S., 27  
Chèze, G., 85  
Cluzeau, T., 11, 81, 86  
Corbacho, E., 173  
Coutsias, E., 192  
Couveignes, J. M., 11, 201

## D

Dali, D., 87  
de Aguilera, M., 301  
de Arriba, F., 173  
de la Villa, A., 37, 239, 240  
del Campo, A. M., 260  
del Rey, Á. M., 37, 239, 240  
Dimovski, I., 92  
Dlotko, P., 291  
Dück, N., 114

## E

Edneral, V., 11, 15, 55, 57  
Escudero, J., 28

## F

Falcón, R., 178  
Fassino, C., 250  
Ferrec, B., 68  
Ferragut, A., 93  
Fortes, I., 41  
Frau, M. D., 289  
Frosini, P., 292  
Fúster Sabater, A., 118

## G

Galán, J. L., 11, 15, 17, 25, 35, 183, 194, 235, 237, 301, 313  
Galán, M. Á., 15, 237  
Gamero, E., 63  
Ganzha, V., 15  
García, A., 37, 239, 240  
García, C., 63  
García, F., 37, 239, 240  
García-Álvarez, A., 194  
Gasull, A., 93  
Geil, O., 120  
Gerdt, V., 11, 15  
Gerdt, V. P., 271, 274  
Gerdt, W., 269  
Giesbrecht, M., 15  
Gogin, N., 184  
Gonçalves, T. M. N., 95  
González Vida, J. M., 11, 15, 299, 309, 312

## H

Henri, F., 238  
Heras, J., 297  
Hermoso, C., 163  
Hernando, A., 11, 161, 187  
Høholdt, T., 122  
Homero Flores, Á., 38  
Hong, H., 15  
Huang, Z., 153

## I

Irtegov, V., 58

## J

Jeffrey, D., 15, 42  
Julia-Diaz, B., 275

## K

Kai, H., 15, 127  
Kaltofen, E., 15  
Khvedelidze, A. M., 271  
Korporal, A., 96  
Kotsireas, I., 11, 15, 19, 107  
Koukouvinos, C., 255  
Kutzler, B., 15

## L

Lewis, R. H., 192  
Lewis, R. L., 15  
Lin, D., 153  
Liñan, R. J., 303  
Liska, R., 15

## M

Maddah, S., 97  
Mansfield, E. L., 95  
Márquez-Corbella, I., 129  
Martin, S., 120  
Martínez, J., 15, 301, 303  
Martínez-Moro, E., 11, 107, 133, 134  
Maruri-Aguilar, H., 11, 243, 261  
Massarenti, A., 212  
Mata, G., 297  
Mencinger, M., 68  
Merino, S., 15, 301, 303, 308, 310, 313  
Mesa, L., 194  
Miszczak, J. A., 276  
Morales de Luna, T., 11, 299, 309, 312  
Muñoz Ruiz, M. L., 11, 15, 299, 309, 312  
Muntingh, G., 163

Munuera, C., 135  
Murillo Mas, A., 290  
Murillo, A., 11, 287  
Myllari, A., 11, 55, 73, 184  
Myllari, T., 73

## N

Navarro, J. F., 74  
Neun, W., 15  
Nicolás, A. P., 133, 134  
Noda, M. T., 15  
Núñez, J., 168

## O

León, W., 135  
Orlowski, A., 281  
Ortega Acosta, S., 309, 312  
Özel, C., 33

## P

Pabón, A. B., 310  
Pacheco, A. M., 293  
Padilla, Y., 15, 237  
Pagani, N., 11, 201, 218  
Palii, Y. G., 271  
Pellikaan, R., 129  
Pérez de Guzmán, I., 41  
Phisanbut, N., 99  
Picard, G., 11, 15, 17, 25, 43  
Piipponen, S., 311  
Pilarczyk, P., 294  
Pineau, K., 15  
Piñero, F., 122  
Pletsch, B., 11, 15, 35  
Polak, M., 137  
Prokopenya, A., 11, 269  
Prokopenya, A. N., 274  
Pujol, J., 142

## Q

Quadrat, A., 86

## R

Raab, C., 100  
Real, P., 11, 287, 289, 293–295  
Recio, T., 164  
Regensburger, G., 11, 81, 96  
Riccomagno, E., 250  
Roanes-Lozano, E., 11, 15, 20, 44, 161, 193, 194  
Robertz, D., 101  
Rodríguez, G., 37, 239, 240

Rodríguez, P., 11, 15, 183, 235, 237, 308, 310  
Rodríguez, R., 207, 237  
Rojas, A., 207  
Romańczuk, U., 144  
Romanovski, V., 11, 55  
Romero, A., 297  
Rosenkranz, M., 11, 81, 99  
Rua, I. F., 133  
Rubio, J., 297  
Rueda, S. L., 102, 219

## S

Sáenz-de-Cabezón, E., 11, 243, 261, 287  
Sánchez Linares, C., 309, 312  
Sánchez, C., 308  
Sánchez, F. J., 308  
Sánchez, S., 41  
Sasaki, T., 15  
Sato, Y., 15  
Savard, G., 43, 238  
Schicho, J., 245  
Schmidt, K., 47  
Sendra, J., 219  
Sendra, J. R., 219, 224  
Sergeraert, F., 297  
Sevilla, D., 224  
Shaska, T., 11, 15, 148, 201, 208, 229  
Shoikova, E., 48  
Shor, C., 148, 229  
Simon, J. J., 109  
Simos, D. E., 255  
Spiridonova, M., 15, 92  
Steinberg, S., 15  
Suárez-Canedo, E., 134  
Sun, Y., 153  
Szanto, A., 15

## T

Tabakin, F., 275  
Takahashi, T., 79  
Tenorio, A. F., 168  
Tran, Q. N., 15  
Tuomela, J., 311  
Turqui, A., 87

## U

Uhler, C., 245, 260, 262  
Ustaoglu, U., 33  
Ustyenko, V., 137, 144, 155  
Uwano, Y., 11, 269, 282

## V

Valverde, A., 41

Varbanoba, E., 241  
Varbanova, E., 11, 35, 48  
Vasiliev, N., 15  
Vassiliev, N., 11, 55  
Vera, J. A., 313  
Vidal, R., 173  
Villanueva, M., 142

## W

Wang, D., 153  
Watt, S., 15  
Wester, M., 11, 15, 35, 161  
Westermann, T., 49  
Windsteiger, W., 15  
Winkler, F., 15  
Wroblewska, A., 155  
Wynn, H. P., 11, 243, 261

## X

Xue, M., 50, 197

## Y

Yamada, M., 127  
Yilmaz, E., 33  
Yoshida, R., 263

## Z

Zafeirakopoulos, Z., 255  
Zeng, F., 142  
Zeng, P., 122  
Zimmermann, K., 114





---

---

# Appendix

---

---



# Spectral sequences for computing persistent homology of digital images\*

Ana Romero, Gadea Mata, Julio Rubio  
University of La Rioja (Spain)

Jónathan Heras  
University of Dundee (UK)

Francis Sergeraert  
University Joseph Fourier (France)

`ana.romero@unirioja.es`

## Abstract

Persistent homology and spectral sequences are two Algebraic Topology tools which are defined by means of a filtration and can be applied to study topological properties of a space at different stages. Both concepts are deeply related, and this relation allows us to use some previous programs developed for computing spectral sequences of filtered complexes to determine now persistent homology. In particular, spectral sequences can be applied to compute persistent homology of digital images, which will allow us to determine relevant features, that will be long-lived on contrast with the “noise” which will be short-lived.

## Keywords

Persistent homology, digital images, spectral sequences.

## 1 Introduction

Persistent homology [4] is an algebraic method for measuring topological features of shapes and functions, with many recent applications such as point cloud data, sensor networks, optical character recognition and protein classification. More concretely, this technique consists in identifying homological features that persist within the different stages of a filtration. On the other hand, spectral sequences [7] are a tool for computing homology groups by taking successive approximations. Both concepts are defined by means of a filtration and are deeply related.

In a previous paper [8], we showed that a slight modification of our previous programs for computing spectral sequences [9] is enough to compute also persistent homology. By inheritance from our spectral sequence program, we obtained for free persistent homology programs applicable to spaces not of finite type (provided they are spaces with effective homology) and with  $\mathbb{Z}$ -coefficients (significantly generalizing the usual presentation of persistent homology over a field). Moreover, our calculations made it possible to detect an error in [4]: the so called “Spectral sequence theorem” [4, p. 171], which shows the relation between spectral sequences and persistent homology, includes a formula which is not correct (see [8] for details).

In this work, we use our spectral sequence programs to compute persistent homology of digital images. This allows us to determine relevant features, that will be long-lived – in the sense that they persist over a certain parameter range – on contrast with the “noise” which will be short-lived. In order to reduce the time of calculations, we can use the combinatorial notion of *Discrete Vector Field* [5]. As a test case, our programs could be applied on a fingerprint database.

---

\*Partially supported by Ministerio de Educación y Ciencia, project MTM2009-13842-C02-01, and by the European Union’s 7th Framework Programme under grant agreement nr. 243847 (ForMath).

## 2 Preliminaries

**Definition 2.1.** Let  $K$  be a simplicial complex. A (finite) *filtration* of  $K$  is a nested sequence of subcomplexes  $K^i \subseteq K$  such that  $\emptyset = K^0 \subseteq K^1 \subseteq K^2 \subseteq \dots \subseteq K^m = K$ .

For every  $i \leq j$  we have an inclusion map on the canonically associated chain complexes  $\text{inc}^{i,j} : C(K^i) \hookrightarrow C(K^j)$  and therefore we can consider the induced homomorphisms  $f_n^{i,j} : H_n(K^i) \rightarrow H_n(K^j)$ , for each dimension  $n$ . The filtration produces then for each dimension  $n$  a sequence of homology groups connected by homomorphisms:

$$0 = H_n(K^0) \rightarrow H_n(K^1) \rightarrow \dots \rightarrow H_n(K^m) = H_n(K)$$

**Definition 2.2.** The  $n$ -th *persistent homology groups* of  $K$ , denoted by  $H_n^{i,j}(K) \equiv H_n^{i,j}$ , are the images of the homomorphisms  $f_n^{i,j}$ :

$$H_n^{i,j} = \text{Im } f_n^{i,j}, \text{ for } 0 \leq i \leq j \leq m$$

The group  $H_n^{i,j}$  consists of the  $n$ -th homology classes of  $K^i$  that are still alive at  $K^j$ . A class  $\gamma \in H_n(K^i)$  is said to be *born* at  $K^i$  if  $\gamma \notin H_n^{i-1,i}$ . It is said to *die* entering  $K^j$  if it merges with an older class as we go from  $K^{j-1}$  to  $K^j$ , that is,  $f_n^{i,j-1}(\gamma) \notin H_n^{i-1,j-1}$  but  $f_n^{i,j}(\gamma) \in H_n^{i-1,j}$ . If  $\gamma$  is born at  $K^i$  and dies entering  $K^j$ , the difference  $j - i$  is called the *persistence index* of  $\gamma$ , denoted  $\text{pers}(\gamma)$ . If  $\gamma$  is born at  $K^i$  but never dies then  $\text{pers}(\gamma) = \infty$ .

If the homology is computed with field coefficients, each group  $H_n^{i,j}$  is a vector space which is determined up to isomorphism by its dimension, and this allows one to represent all persistent homology groups by means of a *barcode* diagram [4]. However, in the integer case one can face extension problems. In order to solve this difficulty, we introduced in [8] a generalization of persistent homology with  $\mathbb{Z}$ -coefficients. This can be done by means of a double filtration which leads to a new (more general) definition of barcode.

**Definition 2.3.** Let  $R$  be a ring, a *spectral sequence*  $E = (E^r, d^r)_{r \geq 1}$  is a sequence of bi-graded  $R$ -modules  $E^r = \{E_{p,q}^r\}_{p,q \in \mathbb{Z}}$ , each provided with a differential  $d^r = \{d_{p,q}^r : E_{p,q}^r \rightarrow E_{p-r,q+r-1}^r\}_{p,q \in \mathbb{Z}}$  of bidegree  $(-r, r-1)$  (satisfying  $d_{p-r,q+r-1}^r \circ d_{p,q}^r = 0$ ) and with isomorphisms  $H(E^r, d^r) \cong E^{r+1}$  for every  $r \geq 1$ . Since each  $E_{p,q}^{r+1}$  is a subquotient of  $E_{p,q}^r$ , one can define the *final groups*  $E_{p,q}^\infty$  of the spectral sequence as the groups which remain after the computation of all successive homologies.

**Theorem 2.4.** [7, p.327] *Let  $C$  be a chain complex with a filtration. There exists a spectral sequence  $E \equiv E(C) \equiv (E^r, d^r)_{r \geq 1}$ , defined by*

$$E_{p,q}^r = \frac{Z_{p,q}^r + C_{p+q}^{p-1}}{d_{p+q+1}^r(Z_{p+r-1,q-r+2}^{r-1}) + C_{p+q}^{p-1}}$$

where  $Z_{p,q}^r$  is the submodule  $Z_{p,q}^r = \{a \in C_{p+q}^p \mid d_{p+q}(a) \in C_{p+q-1}^{p-r}\} \subseteq C_{p+q}^p$ , and  $d_{p,q}^r : E_{p,q}^r \rightarrow E_{p-r,q+r-1}^r$  is the morphism induced on these subquotients by the differential map  $d_{p+q}^r : C_{p+q}^p \rightarrow C_{p+q-1}^{p-1}$ . This spectral sequence converges to the homology groups of  $C$ , that is, there are natural isomorphisms

$$E_{p,q}^\infty \cong \frac{H_{p+q}^p(C)}{H_{p+q}^{p-1}(C)}$$

where  $H_*^p(C)$  is the filtration on the homology groups  $H_*(C)$  induced by the filtration of  $C$ .

## 3 Computing persistent homology by means of spectral sequences

There are some works in the literature which include some comments on the relation between spectral sequences and persistent homology (see for instance [12] and [3]), but the only reference where we have found an explicit formula which relates them is the book ‘‘Computational Topology: An Introduction’’ by Herbert Edelsbrunner and John Harer [4]. Given a filtered simplicial complex  $K$ , the so called ‘‘Spectral sequence theorem’’ ([4, p. 171]) claims that:

The total rank of the groups of dimension  $p + q$  in the level  $r \geq 1$  of the associated spectral sequence equals the number of points in the  $(p + q)$ -th persistence diagram whose persistence is  $r$  or larger, that is,

$$\sum_{p=1}^m \text{rank } E_{p,q}^r = \text{card}\{a \in \text{Dgm}_{p+q}(f) \mid \text{pers}(a) \geq r\}$$

where  $\text{Dgm}_{p+q}(f)$  is an appropriate persistence diagram (see [4, Chap. VII]) and where in the left side  $q$  decreases as  $p$  increases so that the dimension  $p + q$  remains constant.

However, we have detected that the formula in [4] is erroneous because in the spectral sequence side (the left side) there can be more elements than in the persistence (right) side; the formula should be therefore an inequality. To illustrate the error in [4], it suffices to consider as a counterexample a simplicial complex  $K$  generated by the interval  $ab$ , with the filtration given by  $K^1 = \{a, b\}$  and  $K^2 = K$ ; in dimension 1 one has  $E_{2,-1}^1 = \mathbb{Z}$  but there are no classes of persistence at least 1 since the unique element of dimension 1 is not a cycle.

The correct relation between persistent homology and spectral sequences can be expressed by the following theorem:

**Theorem 3.1.** [8] *The total rank of the images of the differential maps in the level  $r \geq 1$  of the spectral sequence equals the number of points in the  $(p + q)$ -th persistence diagram whose persistence is  $r$ :*

$$\sum_{p=1}^m \text{rank } A_{p,q}^r = \text{card}\{a \in \text{Dgm}_{p+q}(f) \mid \text{pers}(a) = r\}$$

where  $A_{p,q}^r = \text{Im}(d_{p+r,q-r+1}^r : E_{p+r,q-r+1}^r \rightarrow E_{p,q}^r) \subseteq E_{p,q}^r$ .

This theorem gives us an algorithm for computing the rank of the persistent homology groups of a filtered simplicial complex from the associated spectral sequence. Let us emphasize that this information about ranks determines (up to isomorphism) the groups  $H_n^{i,j}$  when one works with coefficients over a field  $F$ . Therefore, if we know the groups  $E_{p,q}^r$  and the differential maps  $d_{p,q}^r$  of the spectral sequence of a filtered simplicial complex, thanks to the formula introduced in Theorem 3.1 we can also easily determine the persistent homology groups of  $K$ . If we work with coefficients over  $\mathbb{Z}$ , the previous information about the ranks relating spectral sequences and persistent homology is not sufficient to determine the groups  $H_n^{i,j}$ ; however, we will see later that one can express the groups  $H_n^{i,j}$  in terms of some subgroups appearing in the definition of the spectral sequence, which will allow us to determine  $H_n^{i,j}$  also in the integer case.

In a previous work [9], we developed a set of programs computing spectral sequences associated with filtered chain complexes. These programs were implemented in Common Lisp as a new module for the Kenzo system [2], a computer algebra program developed by the last author of this paper and some coworkers which implements the *effective homology* theory [11] and has made it possible to determine homology and homotopy groups of complicated (infinite) spaces. The new programs for spectral sequences use also the effective homology technique and allow the Kenzo user to determine the different components of spectral sequences of filtered complexes even in some cases where the chain complex has infinite type. Using our programs, and thanks to Theorem 3.1, one can determine in this way the ranks of the groups  $H_n^{i,j}$ .

In fact the computation of the groups  $H_n^{i,j}$  can be directly obtained by a small modification of our algorithms without doing the complete process of computing the corresponding groups and differential maps of the spectral sequence. Let us recall that a group  $E_{p,q}^r$  in the spectral sequence is given by the formula:

$$E_{p,q}^r = \frac{Z_{p,q}^r + C_{p+q}^{p-1}}{d_{p+q+1}(Z_{p+r-1,q-r+2}^{r-1}) + C_{p+q}^{p-1}}$$

We can observe that each class in  $E_{p,q}^r$  is generated by an “almost” cycle of dimension  $p + q$  (a chain whose boundary in  $K^p - K^{p-r}$  is empty but which may have non-empty boundary in  $K^{p-r}$ ), and the elements of  $E_{p,q}^r$  given by a real cycle  $x$  (that is,  $d(x) = 0$ ), correspond to classes of  $H_{p+q}(K^p)$  which are born at  $K^p$  and are still alive at  $K^{p+r-1}$ , and then the persistence indexes of these classes are at least  $r$ .

It is not difficult to observe then that the groups  $H_n^{i,j}$  can also be described as a quotient:

$$H_n^{i,j} = \frac{\text{Ker } d_n \cap C_n^i}{d_{n+1}(Z_{j,n-j+1}^{j-i})} = \frac{Z_{i,n-i}^i}{d_{n+1}(Z_{j,n-j+1}^{j-i})}$$

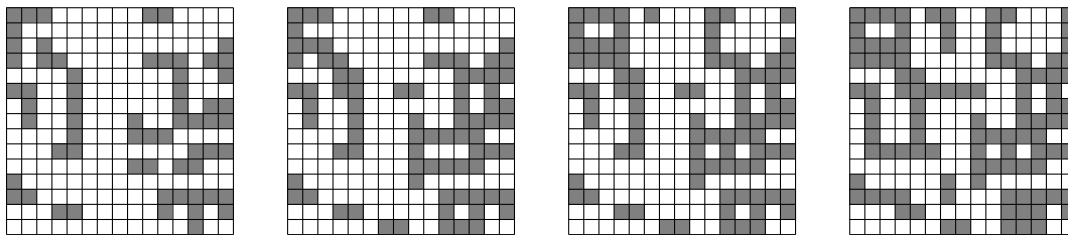


Figure 1: Filtered digital image.

If  $K$  is a finite filtered simplicial complex, then our programs determine the different elements of the associated spectral sequence by means of some elementary operations on matrices. More concretely, the programs determine in particular the subgroups  $Z_{p,q}^r$ ,  $C_{p+q}^{p-1}$  and  $d_{p+q+1}(Z_{p+r-1,q-r+2}^{r-1})$  which appear in the formula of Theorem 2.4 (which can be determined if  $K$  is finite), and then calculate the desired quotient. The groups  $H_n^{i,j}$  are determined in terms of similar subgroups and then it has been very easy to adapt our programs in order to compute also  $H_n^{i,j}$  for finite (filtered) simplicial complexes. It is important to remark that this is also valid in the integer case and this makes it possible to solve the possible extension problems. Our programs can also be applied in the infinite case, where the effective homology method can be used to determine the groups  $H_n^{i,j}$  by means of a *reduction* of the initial chain complex  $C$  to an auxiliary chain complex of finite type (see [8] for details).

## 4 Persistent homology of digital images

Given a digital image, we can naturally associate a simplicial complex  $K$  and compute its homology groups in dimensions 0 and 1 which show respectively the number of connected components and holes that the image contains. If the image is *filtered* (for example, it comes from a stack of images), one can also determine the persistent homology groups which will allow us to determine relevant features, that will be long-lived – in the sense that they persist over a certain parameter range – on contrast with the “noise” which will be short-lived.

Let us consider the filtered image of Figure 1. The final homology groups are  $H_0 = \mathbb{Z}^7$  and  $H_1 = \mathbb{Z}^4$ . We can see the *evolution* of the corresponding homology classes along the four filtration steps by using our programs for computing persistent homology groups based on spectral sequences. For example,  $H_0^{1,4} = \mathbb{Z}^4$ , which means that in dimension 0 there are 4 classes which are born at the first step and are still alive at (the last) step 4:

```
> (prst-hmlg-group K 1 4 0)
Persistent Homology H^{1,4}_0
Component Z
Component Z
Component Z
Component Z
```

Similarly,  $H_1^{2,4} = \mathbb{Z}^2$  means that there are 2 holes at stage 2 which are still alive at step 4:

```
> (prst-hmlg-group K 2 4 1)
Persistent Homology H^{2,4}_1
Component Z
Component Z
```

These same results have been also obtained by a *certified* program, executed inside the Coq proof assistant (this kind of *verified* programs have been developed in the frame of the ForMath European project [1], and have been documented in [6]).

For bigger digital images, we can reduce the time of calculations by using the combinatorial notion of *Discrete Vector Field*, which is an essential component of Forman’s Discrete Morse Theory [5], adapted to the algebraic setting in [10]. As explained in [10], given a digital image, an admissible discrete vector field can be constructed by means of some elementary operations on the differential matrices of the associated chain complex. This vector field produces a *reduction* from the initial (big) chain complex to a (much) smaller one whose homology groups are explicitly isomorphic to the homology groups of the image, so that the computation of these homology groups can be done in a more efficient way.

If we are interested in computing persistent homology groups, we can follow a similar process to construct a discrete vector field and reduce the initial (big) chain complex. In this case the discrete vector field must be compatible with the filtration, which can be done applying the same elementary methods of [10] to the differential submatrices corresponding to each step of the filtration. The vector field so obtained is of course smaller than the non-filtered one, but it usually decreases significantly the number of generators. This vector field produces again a reduction, which in this case is compatible with the given filtration, which implies that the persistent homology groups of the initial image are isomorphic to the persistent homology groups of the reduced one (see [8] for details). Applying now our programs for computing persistent homology to the small chain complex, we can compute the persistent homology groups of big images in an efficient way.

Computation of persistent homology groups of digital images could be applied to study fingerprints. Given a fingerprint image, we could filter it taking at the first step some initial horizontal lines, adding at each stage of the filtration some additional lines and ending with the whole image. This filtration would produce some persistent homology groups. A similar process could be done in the vertical direction, taking successively the columns of the image, producing in that way different persistent homology groups. It seems natural that given two (different) fingerprint images corresponding to the same person, the so obtained persistent homology groups should be similar. Persistent homology could help in this way for fingerprint recognition.

## References

- [1] *ForMath: Formalisation of Mathematics*, <http://wiki.portal.chalmers.se/cse/pmwiki.php/ForMath/ForMath>.
- [2] X. Dousson, J. Rubio, F. Sergeraert, and Y. Siret, *The Kenzo program*, Institut Fourier, Grenoble, 1999, <http://www-fourier.ujf-grenoble.fr/~sergerar/Kenzo/>.
- [3] H. Edelsbrunner and J. Harer, *Persistent homology a survey*, Contemporary Mathematics (2008), 1–26.
- [4] H. Edelsbrunner and J. Harer, *Computational topology: An introduction*, Applied mathematics, American Mathematical Society, 2010.
- [5] R. Forman, *Morse theory for cell complexes*, Advances in Mathematics **134** (1998), 90–145.
- [6] J. Heras, T. Coquand, A. Mörtberg, and V. Siles, *Computing Persistent Homology within Coq/SSReflect*, To appear in ACM Transactions on Computational Logic, 2013.
- [7] S. MacLane, *Homology*, vol. 114, Springer, 1963.
- [8] A. Romero, J. Heras, J. Rubio, and F. Sergeraert, *Defining and computing persistent  $\mathbb{Z}$ -homology in the general case*, Preprint, 2013.
- [9] A. Romero, J. Rubio, and F. Sergeraert, *Computing spectral sequences*, Journal of Symbolic Computation **41** (2006), no. 10, 1059–1079.
- [10] A. Romero and F. Sergeraert, *Discrete Vector Fields and fundamental Algebraic Topology*, Preprint. <http://arxiv.org/abs/1005.5685v1>, 2010.
- [11] J. Rubio and F. Sergeraert, *Constructive Algebraic Topology*, Bulletin des Sciences Mathématiques **126** (2002), no. 5, 389–412.
- [12] A. Zomorodian and G. Carlsson, *Computing persistent homology*, Discrete and Computational Geometry **33** (2005), no. 2, 249–274.