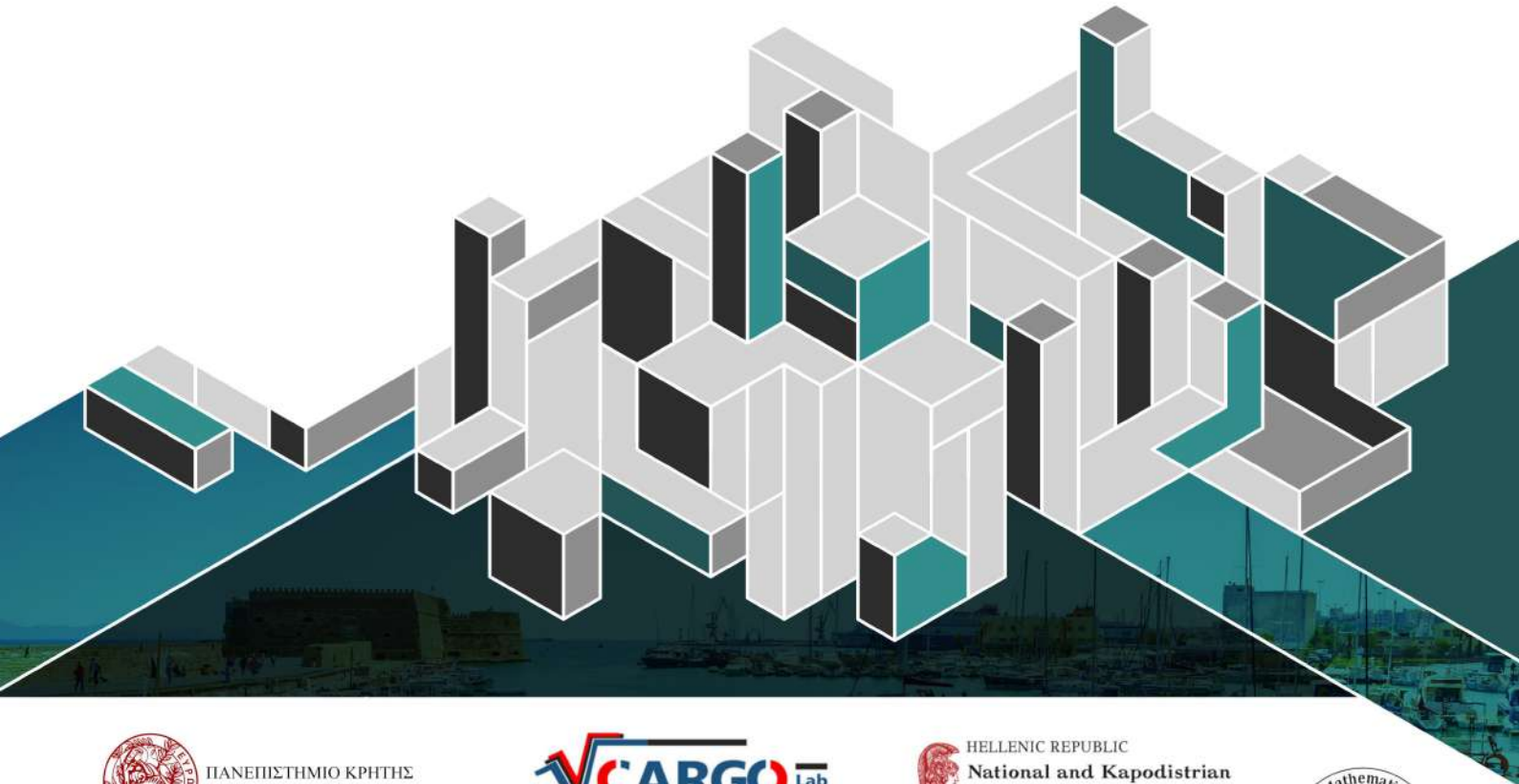
ACA 2025

30th APPLICATIONS of COMPUTER ALGEBRA

BOOK of ABSTRACTS



ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ
UNIVERSITY OF CRETE

DEPARTMENT OF MATHEMATICS

CARGO Lab
Computer Algebra Research Group

Maplesoft
Mathematics • Modeling • Simulation
A Cybernet Group Company

HELLENIC REPUBLIC
National and Kapodistrian University of Athens
EST. 1837

HELLENIC OPEN UNIVERSITY

Hellenic Mathematical Society
1918

Book of Abstracts

30th Applications of Computer Algebra - ACA 2025
https://aca2025.github.io/

14–18 July 2025
Heraklion, Greece

Committees

General Chair

Eleni Tzanaki - University of Crete (Greece)

Program Chairs

Giorgos Kapetanakis - University of Thessaly (Greece)
Zafeirakis Zafeirakopoulos - University of Athens (Greece)

Local Organization Committee

Theodoulos Garefalakis - University of Crete (Greece)

ACA WG co-chairs

Ilias Kotsireas - Wilfrid Lauriel University & CARGO Lab (Canada)
Michael Wester - University of New Mexico (USA)

Scientific Committee

ACA Working Group - `https://math.unm.edu/~aca/ACA/Organizing/WG.html`

ACA conferences

The ACA conference series is devoted to promoting all kinds of computer algebra applications, and encouraging the interaction of developers of computer algebra systems and packages with researchers and users (including scientists, engineers, educators, and mathematicians).

`https://math.unm.edu/~aca/`

ACA'95	May 16–19,	1995	Albuquerque, New Mexico, USA
ACA'96	July 17–20,	1996	RISC-Linz, Hagenberg, Austria
ACA'97	July 24–26,	1997	Wailea, Maui, Hawaii, USA
ACA'98	Aug. 9–11,	1998	Prague, Czech Republic
ACA'99	June 24–27,	1999	El Escorial, Spain
ACA'2000	June 25–28,	2000	Saint Petersburg, Russia
ACA'2001	May 31–June 3,	2001	Albuquerque, New Mexico, USA
ACA'2002	June 25–28,	2002	Volos, Greece
ACA'2003	July 28–31,	2003	Raleigh, North Carolina, USA
ACA'2004	July 22–24,	2004	Beaumont, Texas, USA
ACA'2005	Aug. 8–10,	2005	Nara, Japan
ACA'2006	June 26–29,	2006	Varna, Bulgaria
ACA'2007	July 19–22,	2007	Rochester, Michigan, USA
ACA'2008	July 27–30,	2008	RISC-Linz, Hagenberg, Austria
ACA'2009	June 25–28,	2009	Montréal, Québec, Canada
ACA'2010	June 24–27,	2010	Vlora, Albania
ACA'2011	June 27–30,	2011	Houston, Texas, USA
ACA'2012	June 25–28,	2012	Sofia, Bulgaria
ACA'2013	July 3–6,	2013	Málaga, Spain
ACA'2014	July 9–12,	2014	Bronx, New York City, New York, USA
ACA'2015	July 20–23,	2015	Kalamata, Greece
ACA'2016	Aug. 1–4,	2016	Kassel, Germany
ACA'2017	July 17–21,	2017	Jerusalem, Israel
ACA'2018	June 18–22,	2018	Santiago de Compostela, Spain
ACA'2019	July 16–20,	2019	Montréal, Québec, Canada
ACA'2021	July 23–27,	2021	Athens, Greece (virtual)
ACA'2022	Aug. 15–19,	2022	Gebze, Istanbul, Turkey
ACA'2023	July 17–21,	2023	Warsaw, Poland

ACA'2024	July 24–28,	2024	Havana, Cuba
ACA'2025	July 14–18,	2025	Heraklion, Greece
ACA'2026		2026	Prishtina, Kosovo

List of participants

1. Sergei Abramov - MSU (Russia) (*online*)
2. Marcus Aichmayr - University of Kassel (Germany)
3. Gianira Nicoletta Alfarano - Rennes University (France)
4. Eleftherios Amin-Vlastos - University of Crete (Greece)
5. Meirav Amram (Topol) - SCE (Israel)
6. Ilias Andreou - NKUA, Department of Mathematics (Greece)
7. Nikol Antoniadou - University of Thessaly (Greece)
8. Sara Asensio - University of Valladolid (Spain)
9. Tülay Ayyıldız - Gebze Technical University (Türkiye)
10. Eli Bagno - Jerusalem college of Technology (Israel)
11. Maryam Bajalan - Institute of Mathematics and Informatics, Bulgarian Academy of Sciences (Bulgaria)
12. Joseph Baranoski II - The Catholic University of America (USA)
13. Moulay Barkatou - XLIM- University of Limoges (France)
14. Luca Bastioni - University of South Florida (USA)
15. William Bauldry - ASU (USA)
16. Volodymyr Bavula - University of Sheffield (United Kingdom)
17. Michel Beaudin - École de technologie supérieure (Canada)
18. Matías Bender - Inria - École Polytechnique (France)
19. Cristina Bertone - Università di Torino (Italy)
20. Barbara Betti - Max Planck Institute MiS Leipzig (Germany)
21. Saltanat Bizhanova - Al-Farabi Kazakh National University (Kazakstan)
22. Olivier Bouillot - Gustave Eiffel University (France)
23. Iliya Bouyukliev - Institute of Mathematics and Informatics, BAS (Bulgaria)
24. Stefka Bouyuklieva - St. Cyril and St. Methodius University of Veliko Tarnovo (Bulgaria)
25. Peter Boyvalenkov - Institute of Mathematics and Informatics, Bulgarian Academy of Sciences (Bulgaria)
26. Hadrien Brochet - Inria Saclay (France)
27. Manfred Buchacher - Johannes Kepler Universität Linz (Austria)
28. Van Chien Bui - University of Sciences, Hue University (Vietnam) (*online*)
29. Chiara Castello - University of Campania "L. Vanvitelli" (Italy)
30. Eunice Chan - Chinese University of Hong Kong, Shenzhen (China)
31. Steven Charlton - Max Planck Institute for Mathematics, Bonn (Germany)
32. Maria Chatzikyriakou - National and Kapodistrian University of Athens (Greece)
33. Cyrille Chenavier - Limoges University (France)

34. Maria Chlouveraki - National and Kapodistrian University of Athens (Greece)
35. Frédéric Chyzak - Inria (France)
36. Francesca Cioffi - Università di Napoli Federico II, Dipartimento di Matematica e Applicazioni (Italy)
37. Thierry Combot - Université de Bourgogne (France)
38. Rob Corless - Western University (Canada)
39. Florent Corniquel - Sorbonne University and INRIA Paris (France)
40. Annie Cuyt - University of Stirling and University of Antwerp (United Kingdom and Belgium)
41. Lucas Da Silva Reis - Universidade Federal de Minas Gerais (Brazil)
42. Thierry Noah Dana-Picard - Jerusalem College of Technology (Israel)
43. Benedek Dombos - University of Geneva (Switzerland)
44. Peter Dragnev - Purdue University Fort Wayne (USA)
45. Gérard H. E. Duchamp - IHP and LIPN, Paris Sorbonne City (France) (*online*)
46. Mariya Dzhumalieva-Stoeva - (Bulgaria)
47. Hélène Décoste - Collège Lionel-Groulx (Canada)
48. Ioannis Emiris - ATHENA RC and University of Athens (Greece)
49. Jean-Yves Enjalbert - Lycée Jean-Batiste Corort, Savigny sur Orges (France)
50. Cristina Fernández-Córdoba - Universitat Autònoma de Barcelona (Spain)
51. Florian Fürnsinn - University of Vienna (Austria)
52. Theodoulos Garefalakis - University of Crete (Greece)
53. Özhan Genç - Jagiellonian University (Poland)
54. Jürgen Gerhard - Maplesoft (Canada)
55. Francesco Ghiandoni - University of Perugia (Italy)
56. Khalil Ghorbal - INRIA (France)
57. Mark Giesbrecht - University of Waterloo (Canada)
58. Richard Golnik - Leipzig University (Germany)
59. Gal Goren - Technion - Israel Institute of Technology (Israel)
60. Robert Green - University of Colorado, Boulder (USA)
61. Margherita Guida - Università di Napoli Federico II (Italy)
62. Alexandre Guillemot - Inria Saclay (France)
63. Domingo Gómez-Pérez - Universidad de Cantabria (Spain)
64. Burcu Gülmez Temür - Atılım University (Türkiye)
65. Cem Güneri - Sabancı University (Türkiye)
66. Bryan Hernandez - University of the Philippines Diliman (Philippines)
67. Vincel Hoang Ngoc Minh - University of Lille (France)
68. Clemens Hofstadler - Johannes Kepler University (Austria)
69. Bo Huang - Beihang University (China)
70. Jack Jansma - University of Stellenbosch (South Africa)
71. David Jeffrey - University of Western Ontario (Canada)
72. Antonio Jiménez-Pastor - Universidad Politécnica de Madrid (Spain)
73. Fredrik Johansson - Inria Bordeaux (France)
74. Elisa Junghans - Ilmenau University of Technology (Germany)
75. Daniel Juteau - CNRS / Université de Picardie Jules Verne (France)
76. Tekgül Kalaycı - Alpen-Adria-Universitat Klagenfurt (Austria)
77. Yuta Kambe - Mitsubishi Electric (Japan)
78. Giorgos Kapetanakis - University of Thessaly (Greece)

79. Alexandros Karakonstantakis - Department of Mathematics and Applied Mathematics (Greece)
80. Manuel Kauers - Johannes Kepler UniversityLinz (Austria)
81. Kohei Kitamura - The University of Osaka (Japan) (*online*)
82. Nao Komiyama - Osaka university (Japan) (*online*)
83. Chieko Komoda - National Institute of Technology, Kurume College (Japan)
84. Ilias Kotsireas - WLU (Canada)
85. Ryszard Kozera - Warsaw University of Life Sciences - SGGW (Poland)
86. Peter Krug - Universität Kassel (Germany)
87. Yasuyuki Kubo - Yuge KOSEN (Japan)
88. Roberto La Scala - Università degli Studi di Bari (Italy)
89. George Labahn - University of Waterloo (Canada)
90. Gilbert Labelle - Université du Québec à Montréal (Canada)
91. Grégoire Lecerf - CNRS & École polytechnique (France)
92. Wen-shin Lee - University of Stirling (United Kingdom)
93. Alexander Levin - The Catholic University of America (USA)
94. Robert Lewis - Fordham University (USA)
95. Julia Lieb - TU Ilmenau (Germany)
96. Giovanni Longobardi - University of Naples Federico II (Italy)
97. Maria Loukaki - University of Crete (Greece)
98. Yota Maeda - TU Darmstadt/Tohoku University (Germany/Japan)
99. Stelios Mathioulakis - University of Crete (Greece)
100. Aristeidis Meramveliotakis - University of Crete (Greece)
101. Angeliki-Aikaterini Metallinou - University of Athens (Greece)
102. Tobias Metzlaff - LAAS-CNRS (France)
103. Andrzej Mizera - University of Warsaw; IDEAS Research Institute (Poland)
104. Atsushi Mochizuki - Institute for Life and Medical Sciences, Kyoto University (Japan)
105. Michael Monagan - Fraser University (Canada)
106. Lucia Moura - University of Ottawa (Canada)
107. Yulia Mukhina - LIX, CNRS, École polytechnique, Institute Polytechnique de Paris (France)
108. Dinushi Munasinghe - National and Kapodistrian University of Athens (Greece)
109. Abhiram Natarajan - University of Warwick (United Kingdom)
110. Alessandro Neri - University of Naples Federico II (Italy)
111. Quoc Hoan Ngo - HaNoi University of science and technology (Vietnam) (*online*)
112. Vu Nguyen Dinh - University of Science and Technology of Hanoi (Vietnam) (*online*)
113. Koji Nishiura - National Institute of Technology, Fukushima College (Japan)
114. Arthur Norman - Trinity College, Cambridge (United Kingdom)
115. Anthony O'Hare - University of Stirling (United Kingdom)
116. Jakob Obrovsky - Johannes Kepler University Linz (Austria)
117. Matthias Orth - KU Leuven (Belgium)
118. Arkadiusz Orłowski - Instytut Informatyki Technicznej SGGW w Warszawie (Poland)
119. Ferruh Ozbudak - Sabanci University (Türkiye)
120. Christos Pallikaros - University of Cyprus (Cyprus)
121. Garrett Paluck - Simon Fraser University (Canada)
122. Daniel Panario - Carleton University (Canada)
123. Maria Papadopoulou - University of Crete (Greece)
124. Valentina Pepe - Sapienza University of Rome (Italy)
125. Simone Pesatori - Università degli Studi Roma Tre (Italy)

126. Götz Pfeiffer - University of Galway (Ireland)
127. Veronika Pillwein - Johannes Kepler University - RISC (Austria)
128. Despoina Maria Pitsoka - University of Thessaly (Greece)
129. Tefjol Pllaha - University of South Florida (USA)
130. Alexander Prokopenya - Warsaw University of Life Sciences (Poland)
131. Kostas Psaromiligkos - Université Clermont Auvergne (France)
132. Long Qian - Carnegie Mellon University (USA)
133. Ovidiu Radulescu - University of Montpellier (France)
134. Varadharaj RaviSrinivasan - Indian Insititute of Science Education and Research Mohali (India)
135. Georg Regensburger - University of Kassel (Germany)
136. Daniel Robertz - RWTH Aachen University (Germany)
137. Julien Roques - Université Lyon 1 (France)
138. Fabrice Rouillier - Inria (France)
139. Joao Ruiz - Institut de Mathématiques de Jussieu (IMJ-PRG) / INRIA (France)
140. Pietro Sabatino - Institute for High Performance Computing and Networking (ICAR-CNR) (Italy)
141. AmirHosein Sadeghimanesh - Coventry University (United Kingdom)
142. Elena Sammarco - Università degli studi Roma Tre (Italy)
143. Haiduke Sarafian - Pennsylvania State University (USA)
144. Michael Schaller - University of Zürich (Switzerland)
145. Karsten Schmidt - Schmalkalden University of Applied Sciences (Germany)
146. Werner M. Seiler - Kassel University (Germany) (*online*)
147. Ramonika Sengupta - Eindhoven University of Technology (The Netherlands)
148. John Sheekey - University College Dublin (Ireland)
149. Dimitris Simos - Paris Lodron University of Salzburg and Salzburg University of Applied Sciences (Austria)
150. Magdalena Skrzypiec - Maria Curie-Sklodowska University (Poland)
151. Valentino Smaldore - Università degli Studi di Padova (Italy)
152. Henning Stichtenoth - Sabanci University (Türkiye)
153. Arne Storjohann - University of Waterloo (Canada)
154. Masaki Suzuki - National Institute of Technology, Numazu College (Japan)
155. Antonia Syrigou - University of Crete (Greece)
156. Setsuo Takato - KeTCindy Center (Japan)
157. Christos Tatakis - University of Western Macedonia, Department of Mathematics (Greece)
158. Sasaki Tateaki - University of Tsukuba (Japan)
159. Bertrand Teguia Tabuguia - University of Oxford (United Kingdom)
160. Máté László Telek - Max Planck Institute for Mathematics in the Sciences (Germany)
161. Piedad Tolmos - Juan Carlos University (Spain)
162. Alev Topuzoglu - Sabanci University (Türkiye)
163. Sofia Triantafyllou - University of Crete (Greece)
164. Rocco Trombetti - Università degli Studi di Napoli Federico II (Italy)
165. Manos Tsagkarakis - University of Crete (Greece)
166. Elias Tsigaridas - Inria Paris (France)
167. Daniel Tsirkin - JCT Israel (Israel)
168. Eleni Tzanaki - University of Crete (Greece)
169. Ali K. Uncu - University of Bath (United Kingdom)

170. Nicola Vassena - Leipzig University (Germany)
171. Carlos Vela Cabello - Universität St Gallen (Switzerland)
172. Irene Villa - University of Trento (Italy)
173. Raffaele Vitolo - University of Salento (Italy)
174. Maria Vitsilaki - University of Crete (Greece)
175. Panagiota Vitsiou - University of Thessaly (Greece)
176. Qiang (Steven) Wang - Carleton University (Canada)
177. Dingkang Wang - Academy of Mathematics and Systems Science, Chinese Academy of Sciences (China)
178. Qingwen Wang - Shanghai University (China)
179. Stephen Watt - University of Waterloo (Canada)
180. Martin Weimann - University Caen Normandy (France)
181. Shachar Weinbaum - Technion - Israel Institute of Technology (Israel)
182. Michael Wester - University of New Mexico (USA)
183. Mengyan Xie - Shanghai Ocean University (China)
184. Jing Yang - Guangxi Minzu University (China) (*online*)
185. Irini Yzeiraj - University of Crete (Greece)
186. Zafeirakis Zafeirakopoulos - National and Kapodistrian University of Athens (Greece)
187. Thekla Zampeta - University of Thessaly (Greece)
188. Chia Zargeh - Modern College of Business and Science (Oman) (*online*)
189. Yang Zhang - University of Manitoba (Canada)
190. Yi Zhang - Xi'an Jiaotong-Liverpool University (China)
191. Xiaodong Zhang - Shanghai Jiao Tong University (China) (*online*)
192. Jianqiang Zhao - The Bishop's School (USA)
193. Stela Zhelezova - Institute of Mathematics and Informatics, BAS (Bulgaria)
194. Lihong Zhi - Academy of Mathematics and Systems Science (China)
195. Joris van der Hoeven - CNRS (France)
196. Buket Özkaya - Middle East Technical University (Türkiye)

Foreward

Welcome to the 30th annual conference on Applications of Computer Algebra. This series was founded by Stanly Steinberg and Michael Wester in 1995, with the first conference being held May 16–19 in Albuquerque, New Mexico, USA at the University of New Mexico. At the time, Stan saw a need for a computer algebra applications conference, and enlisted Michael, his newly minted PhD, to become co-chair. We never dreamed that this first meeting would spawn 29 more conferences, and are both amazed and pleased.

ACA has been a successful experiment. As espoused in the online *ACA Traditions*,

> ACA is a semi-chaotic organization that survives on volunteerism and not being overly encumbered by too many rules. The primary mission of ACA conferences is to foster interaction among a diverse group of developers and users in a variety of disciplines. Interaction can occur on many different levels at once (technical, administrative, social) and all are important in establishing relationships that will benefit the community, immediately and over time. All these levels should be taken into account when preparing a conference (high quality talks, good conference organization, social activities). However, we also discourage formalizing too many specifics and prefer letting the conference chairs decide how to best implement the above goals.

ACAs have been held in a variety of locations around the world, reflecting the diversity of the participants that come to these meetings:

North America
: Canada [2], Cuba, United States [Hawaii, Michigan, New Mexico (2), New York, North Carolina, Texas (2)]

Europe
: Albania, Austria [2], Bulgaria [2], Czechia, Germany, Greece [3], Poland, Russia, Spain [3]

Asia
: Israel, Japan, Turkey

worldwide
: virtual

The current meeting, ACA 2025, to be held in Heraklion, Crete, Greece, looks to have possibly a record number of sessions proposed (18) and an experienced cast of organizers: Eleni Tzanaki (general chair); George Kapetanakis and Zafeirakis Zafeirakopoulos (program chairs). There are

also four invited speakers (Gianira Nicoletta Alfarano, Ioannis Emiris, Daniel Panario, Veronika Pillwein). The co-chairs of the ACA Working Group (ACA-WG), who provide continuity to the conference series, are Michael Wester and Ilias Kotsireas.

An important aspect of the ACA conferences series is the recently established award for early career researchers, namely the ACA-ERA. The year 2025 marks the 5th anniversary of this award. The award consists of a certificate and a financial stipend. The award has been generously sponsored by:

- CARGO Lab, Wilfrid Laurier University, Waterloo, Ontario, Canada
- Maplesoft, Waterloo, Ontario, Canada
- Wolfram Research, Champaign, Illinois, USA
- ACM SIGSAM, New York, USA
- Center for Computer Mathematics, China
- SBA Research, Austria

On a final note, 2025 is a numerically interesting year:

- $2025 = 45^2 = 5^2 \cdot 9^2$
- $2025 = 27^2 + 36^2 = 40^2 + 20^2 + 5^2$
- $2025 = \left(\sum_{n=1}^{9} n\right)^2 = \sum_{n=1}^{9} n^3$
- $2025 = \sum_{n=1}^{45} (2n - 1)$

And so, ACA 2025, will be a symbolically (and symbolically-numerically) interesting meeting!

Michael J. Wester, *Stanly L. Steinberg* and *Ilias Kotsireas*

Acknowledgments

The ACA 2025 conference was **thoroughly organized** by

- University of Crete,
- University of Thessaly,
- National and Kapodistrian University of Athens,
- Εταιρία Έρευνας και Πράξης,

and **generously sponsored** by

- Department of Mathematics, University of Thessaly,
- CARGO Lab,
- Maplesoft,
- Hellenic Mathematical Society,
- Hellenic Open University.

Contents

Plenary talks

Skew-polynomial rings and algebraic coding theory

Gianira N. Alfarano
Rennes University, France

Cyclic codes are one of the most studied families of block codes in classical coding theory, because they provide the algebraic framework for the construction of codes such as Reed-Solomon and BCH codes. A natural generalization of these codes are the so-called skew-cyclic codes. They are based on skew-polynomial rings in one indeterminate. The only difference from a commutative polynomial ring is that in the skew version the indeterminate does not commute with its coefficients. In this talk, we will first discuss the applications of the theory of skew-polynomial rings to algebraic coding theory. We will discuss some recent results pertaining to the distance of skew-cyclic codes in Hamming, rank and sum-rank metrics. The presentation is based on literature on skew-polynomial rings by Ore (1933) and Lam/Leroy (between 1988 and 2012), as well as literature on skew-cyclic codes by Boucher/Ulmer et al. (between 2007 and 2014), and on joint work with Lobillo, Neri and Wachter-Zeh (2021-2022).

References

[1] G.N. Alfarano, F.J. Lobillo, A. Neri, A. Wachter-Zeh. Sum-rank product codes and bounds on the minimum distance. Finite Fields Appl. 80, 102013, 2022.
[2] D. Boucher and F. Ulmer. Coding with skew polynomial rings. J. Symb. Comput., 44:1644–1656, 2009.
[3] D. Boucher and F. Ulmer. Self-dual skew codes and factorizations of skew polynomials. J. Symb. Comput., 60:47–61, 2014.
[4] D. Boucher, W. Geiselmann, and F. Ulmer. Skew-cyclic codes. AAECC, 18:379–389, 2007.
[5] T. Y. Lam and A. Leroy. Vandermonde and Wronskian matrices over division rings. J. Algebra, 119:308–336, 1988.
[6] A. Leroy. Noncommutative polynomial maps. J. Algebra Appl., 11(4), 2012.
[7] O. Ore. Theory of non-commutative polynomials. Annals Math., 34:480–508, 1933.
[8] Ball, A. Blokhuis, A. Gács, P. Sziklai, Zs. Weiner. On linear codes whose weights and length have a common divisor. Adv. Math., 211 (2007) 94–104.

A sparse overview of sparse elimination

Ioannis Emiris
ATHENA RC and University of Athens, Greece

From its origins in the 1970's until today, sparse, or toric, elimination theory has evolved into a standard approach in algebraic variable elimination, offering new root counts as well as new algorithmic methods important in bounding complexity and leading to practical results for polynomial system solving. The theory's connections to convex geometry, linear algebra, algebraic combinatorics, and tropical geometry offer avenues for further investigation. In this talk we survey complexity and algorithmic aspects, while including some recent results and some open questions for future research.

Iterating Generalized Cyclotomic Mappings of Finite Fields

Daniel Panario
Carleton University, Canada

When we iterate functions over finite structures, there is an underlying natural functional graph. For a function f over a finite field $\mathbb{F}_q$, this graph has q nodes and a directed edge from vertex a to vertex b if and only if $f(a) = b$. It is well known, combinatorially, that functional graphs are sets of connected components, components are directed cycles of nodes, and each of these nodes is the root of a directed tree.

Some functions over finite fields when iterated present strong symmetry properties. These symmetries allow mathematical proofs of some dynamical properties such as the period and preperiod of a generic element, (average) "rho length" (number of iterations until a cycle is formed), number of connected components, cycle lengths, and permutational properties (including the cycle decomposition).

We briefly survey the main problems and results in this area. Then, we concentrate on the functional graph of generalized cyclotomic mappings of finite fields. These are a natural and manageable generalization of monomial functions. We study periodic points, cycle structure, and rooted trees attached to periodic points. We provide both theoretical results on the structure of their functional graphs as well as algorithms for solving basic problems, such as parametrizing the connected components of the graph, or describing the structure of a connected component given by a representative vertex.

Based on the following papers:

1. "A survey on iterations of mappings over finite fields", R. Martins, D. Panario and C. Qureshi; Radon Series on Computational and Applied Mathematics, de Gruyter, 23, 135–172, 2019.

2. "Functional graphs of generalized cyclotomic mappings of finite fields", A. Bors, D Panario and Q. Wang; `https://arxiv.org/abs/2304.00181`, 219 pages.

Sequences and series beyond holonomic

Veronika Pillwein
Johannes Kepler University - RISC, Austria

Holonomic objects, whether infinite sequences or formal power series, can be represented with finite data, are closed under several operations, and form a class for which many algorithms have been developed and implemented. These expressions appear in many applications in Mathematics, Computer Science or Natural Sciences, but there is also a world outside of holonomic.

In this talk, we first recall some of the classical algorithms before moving on to the non-holonomic universe. We present some subsets, that can be represented with finite data, are closed under certain operations and/or form a class for which algorithms have been recently developed and implemented.

SPECIAL SESSION 1

Computer Algebra in Education

Education has become one of the fastest growing application areas for computers in general and computer algebra in particular. Computer Algebra Systems (CAS) and Dynamical Geometry Systems (DGS) make for powerful teaching and learning tools within mathematics, physics, chemistry, biology, economics, etc. Among them are: (a) commercial "heavy weights" such as Casio ClassPad 330, Magma, Maple, Mathematica, MuPAD, TI NSpire CAS, and (b) free software/open source systems such as Axiom, Desmos, Euler, Fermat, wxMaxima, Reduce, and rising stars such as GeoGebra, SageMath, SymPy and Xcas (the swiss knife for mathematics), not to mention systems like Derive (discontinued commercially since 2007) and the essential WolframAlpha, which are important resources for users of symbolic systems.

The goal of this session is to exchange ideas, discuss classroom experiences, and to explore significant issues relating to CAS tools/use within education. Subjects of interest for this session will include new CAS-based teaching/learning strategies, curriculum changes, new support materials, assessment practices from all scientific fields, and experiences of joint use of applied mathematics and CAS including dynamic geometry.

Generative Artificial Intelligence has entered the world very strongly. The Education community has begun to explore the pros and cons of this new technology. We also welcome experiments and research about its usage, either alone or in collaboration with CAS and DGS.

We emphasize that all levels of education are welcome, from high school to university, and that all domains are welcome, including teacher training, engineer training, etc.

Session organizers

- Michel Beaudin (ETS, Canada)
- Michael Wester (University of New Mexico, USA)
- Thierry (Noah) Dana-Picard (Jerusalem College of Technology, Israel)
- Alkis Akritas (University of Thessaly, Greece)
- José Luis Galán García (Universidad de Málaga, Spain)
- Elena Varbanova (Technical University of Sofia, Bulgaria)
- Eli Bagno (Jerusalem College of Technology, Israel)

1.1 Automatic Grading of Online Graph Plotting Problems

Chieko Komoda
National Institute of Technology, Kurume College, Japan

In mathematics education, students are frequently tasked with drawing graphs that accurately represent given mathematical formulas. This paper presents a novel method for the automated grading of student-drawn graphs within a learning management system (LMS). Our work specifically utilized Bézier curves and Oshima spline curves (a variant derived from Bézier curves), developing assessment questions with the aid of the dynamic geometric graph software "KeTCindy".

1.2 Educational Applications of Solving Sangaku Problems by the MNR Method with Maxima

Koji Nishiura
National Institute of Technology, Fukushima College, Japan

This paper explores the educational potential of solving traditional Japanese Sangaku problems using the MNR method in conjunction with the computer algebra system Maxima. Sangaku, geometric problems inscribed on wooden tablets during the Edo period, provide rich and challenging content for mathematical exploration. The MNR method allows for symbolic representation of geometric relationships within triangles, enabling efficient solution strategies through Maxima. By engaging students in the process of formulating problems, interpreting algebraic output, and visualizing geometric structures, this approach fosters deeper mathematical understanding and programming literacy. We demonstrate how this method can contribute to developing students' problem-solving skills, logical reasoning, and sustained interest in mathematics through culturally significant and intellectually stimulating content.

1.3 CAS and Improper Integral - a case study

Magdalena Skrzypiec
Maria Curie-Sklodowska University, Poland

The problem of teaching improper integrals with CAS is not new. I was considered for example in [1], [2] and [3]. During this talk examples of two improper integrals

$$\int_0^\infty \int_0^\infty \sin(x^2+y^2)\,dxdy \quad \text{and} \quad \int_0^\infty \int_0^\infty \cos(x^2+y^2)\,dxdy$$

will be considered. We will discuss the problem of convergence of these integrals. We will also analyze and discuss results obtained using different CAS and AI tools.

References

[1] G. Aguilera, J. L. Galán, M. Á. Galán, Y. Padilla, P. Rodríguez, R. Rodríguez. Teaching improper integrals with CAS, *ACA*, 2015.

[2] J. L. Galán-García, G. Aguilera-Venegas, M. Á. Galán-García, P. Rodríguez-Cielos, I. Atencia-Mc.Killop. Improving CAS capabilities: new rules for computing improper integrals, *Appl. Math. Comput.* 316 (2018), 525–540.

[3] J. L. Galán-García, G. Aguilera-Venegas, M. Á. Galán-García, P. Rodríguez-Cielos, I. Atencia-Mc.Killop, Y. Padilla-Domínguez, Yolanda, R. Rodríguez-Cielos. Enhancing Cas improper integrals computations using extensions of the residue theorem, *Adv. Comput. Math.* 45 (2019), no. 4, 1825–1841.

1.4 An educational proposal to interpret linear systems

Margherita Guida
Università di Napoli Federico II, Italy

During the process of learning mathematics in secondary education, some students encounter difficulties with various algebraic and geometrical concepts, for example they have problems to interpret and to solve linear systems. Different studies indicate that the student's comprehension of these knowledges is mainly technical, rote-based and non-meaningful. In this talk I suggest the design and the implementation of an educational proposal focused on improving student's comprehension of these arguments. In particular, I intend to present Cimmino's reflection algorithm for the numerical solution of linear systems. This method is striking because of its simplicity and elegance. Unlike so many other algorithms for solving linear equations, it is based on a geometrical construction rather than on algebraic manipulations. Moreover, a probabilistic argument is also devised to improve the Cimmino's algorithm. This subject is an opportunity to show students how linear algebra can interact fruitfully not only with algebra, geometry, and numerical analysis, but also with probability theory and methods.

At the time it was conceived, the greatest attraction of the method was probably the fact that the method is always convergent. For a long time (several decades) Cimmino's method, in spite of its virtues, did not see much use. Since the early 1980s, though, an increasing number of authors have returned to Cimmino's method. In fact, it has been shown that this algorithm works well in parallel computing, in particular for applications in the area of image reconstruction via X-ray tomography. Over the years, it was applied in different areas, for example: convex mathematical programming, fast adaptation of radiation therapy planning, filtering in signal processing, solution of "inverse problems"in medical physics.

References

[1] M. Benzi. Gianfranco Cimmino's Contributions to Numerical Mathematics, *Rend. Acc. Sc. Fis. Mat. Napoli*, (4) 89 (2022), pp.73-98.
[2] G. Cimmino. An unusual way of solving linear systems, *Atti Accad. Naz. Lincei. Math.*, Ser. VIII, LXXX, N. 1-2, (1986), pp. 6–7.
[3] M. Guida and C. Sbordone. The reflection method for the numerical solution of linear systems, *SIAM REVIEW - Section: Education*, Vol. 65, No. 4, (2023), pp.1137-1151.

1.5 Cooperation of KeTCindyJS and Maxima

Masaki Suzuki
National Institute of Technology, Numazu College, Japan

This paper presents some HTML teaching materials created through the integration of KeTCindyJS and Maxima. KeTCindyJS is suitable for mathematical visualization, but errors occur in the results because the operations are numerical calculations. Therefore, the HTML teaching materials were created by entrusting the computational processing to Maxima.

1.6 Mathematical Experiments for Mathematics Majors

Michael Monagan
Simon Fraser University, Canada

At Simon Fraser University I teach a second year course entitled "Computing with Calculus". The course is a required course for all mathematics majors and applied mathematics majors. The prerequisites are an integral calculus course and a first programming course. The course covers one variable calculus, a little bit of multivariate calculus (partial derivatives) and some modelling with first order systems of differential equations. Students attend one lecture (one hour) and one lab (one hour) per week for 12 weeks.

One goal of the course is to get mathematics majors to use a mathematical software package (I use Maple) to perform a variety of calculations for calculus. Obviously, we want the students to be able to calculate indefinite integrals and definite integrals, solve (systems) of algebraic equations, and solve differential equations. We want them to be able to do these calculations both exactly, and numerically.

A second goal is to teach the students to visualize everything they are doing. Maple and Mathematica have a wide range of graphics capabilities. From a simple plot of $f(x)$ to plotting an implicit surface $f(x, y, z) = 0$ to creating field plots for systems of differential equations.

The third goal is to teach the students how to do a "mathematical experiment". The experiment may be to disprove a conjecture, check a formula, find an optimum solution, or generate an animation of a mathematical object. Doing mathematical experiments usually requires programming, hence the programming prerequisite. Indeed the course provides students a first opportunity to practice their programming skills on mathematical problems instead of more computing problems.

In the talk I will share six mathematical experiments (one per assignment) that I've found to be interesting and instructive for students. The first experiment is the prime number race (See [1]). This can be done with a single for loop that loops through the primes and counts how many primes are congruent to 1 mod 4 and how many are congruent 3 mod 4. The experiment is to determine which count win's the race? The 1's or the 3's?

References

[1] Andrew Granville and Greg Martin. Prime Number Races. *The American Mathematical Monthly* **113**(1):1–33, 2018.

1.7 Questions and ideas from deceased colleagues that help us carry on

Michel Beaudin
École de technologie supérieure, Canada

Having been involved, over the past 30 years, in several conferences on the use of computer algebra systems in mathematics education (notably, the TIME, USACAS, T^3IC conferences and the Education session of the ACA conferences), I have met several colleagues from whom I have learned a lot. The recent unexpected deaths of some of them, within only 15 months of each other, have upset many of us. An original way to honor their memory is to show how, starting from their personal mathematical concerns – quite different – this can lead to an attempt to answer the

following question: how, surrounded today by all this technology and artificial intelligence, can we continue to teach mathematics to the current clientele of students? The examples presented will be for some mathematics courses that engineering students must take.

1.8 Collaboration with ChatGPT for research and teaching in algebraic combinatorics

Eli Bagno and Thierry (Noah) Dana Picard
Jerusalem College of Technology, Israel

As soon as a new technology is launched, the world of education checks its abilities and possible pedagogical usages. Since ChatGPT has been launched in 2023, researchers have analyzed its affordances, and also compared them with other technologies [5]. Previously, we analyzed the capabilities of ChatGPT as a teaching assistant in Linear Algebra, at senior High-School and undergraduate levels [2] and [3]. Currently, we explore ChatGPT's abilities as a research assistant, this time in algebraic combinatorics. We report about our experience with using artificial intelligence tools to conduct genuine mathematical research. We were surprised by the results, and the collaboration with our research partners benefited greatly from integrating AI tools into our work.

Typically, computers are used to perform calculations that were once done by hand. This involves programming, and the problem with programming is that, with every small change in the properties you are studying, you have to change the code.

AI can solve that problem for you. You simply tell it what you want it to do — just like you would do to a fellow mathematician, and it computes for you.

Sometimes, AI serves not only as a research assistant but also as an expert. We asked it to "read" a central book in algebraic combinatorics and we asked it to explain to us a theorem presented in the book, and we hardly understood it. After some fine tuning, the AI excelled in explaining to us the context of the theorem and also created some helpful examples, which were not taken from the text; see Fig. 1.1.

When you read a mathematical theorem in a book and try to understand it, you may come across concepts you do not know or do not remember. If you have an expert in the field in your vicinity, you can ask him for help. If you are alone, you will have no choice but to flip through the book and find it. Then return to the place you were reading.

Here, the AI can be helpful. When requested to explain to us a notion that had already appeared in the text, it gave us an excellent answer. Apparently, the bot read the book.

In our talk, we will describe the different sessions with the AI, the examples it provided, and how this improved our AI literacy, making the usage of the new technology an integral part of the newly acquired mathematical knowledge (see [1]). The OECD defined the 4 C's of 21st Century Education: Communication, Collaboration, Critical Thinking and Creativity (see Fig. 1.2).

They meant Communication, Collaboration between humans. In [8] and [10], communication is extended to man-machine and machine-machine. Here we experienced new endeavors with man-and-machine. Critical thinking applied for [3] and after, enabled us to develop an efficient dialog with the bot. Communication with the bot is supposed to be in natural language; nevertheless there are some rules to follow in order for it to be efficient and to avoid the strange/false answers we experienced in the past, and still experience in some cases. We must mention that a 5th C has to be added to the previous list, namely **Curiosity**, without which Creativity may be limited. This

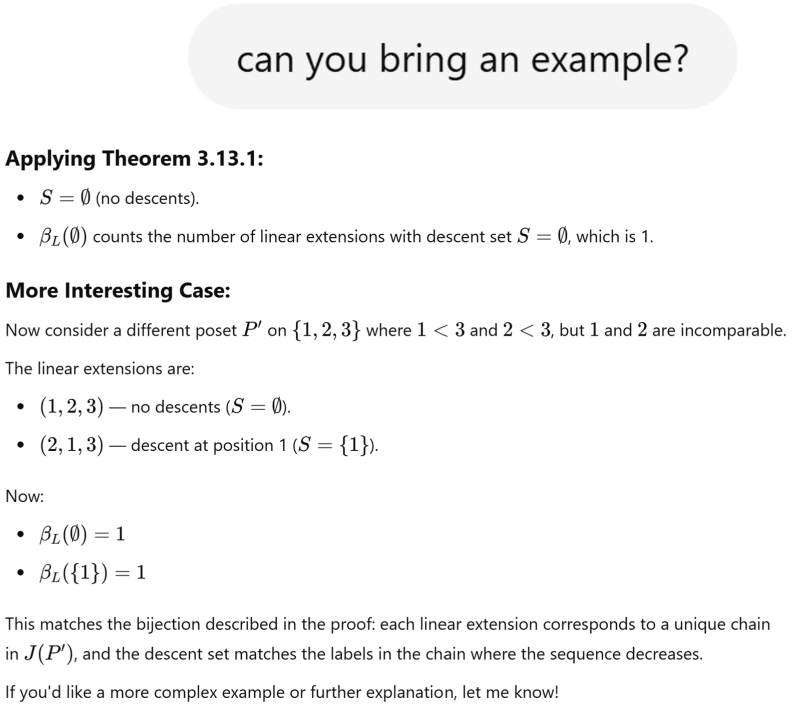


Figure 1.1: Examples ChatGPt

issue has been addressed briefly in [7] and [9] for plane algebraic geometry and related topics; it is a must for the exploration of the new abilities offered by AI.

In a later step, we will discuss how to apply our explorations and discovery towards a didactic transposition (in the spirit of [6]) and a useful work with students.

References

[1] M. Artigue (2002). *Learning mathematics in a CAS environment: The genesis of a reflection about instrumentation and the dialectics between technical and conceptual work*, International Journal of Computers for Mathematical Learning **7(3)**, 245-–274.

[2] E. Bagno, T. Dana-Picard and S. Reches: *ChatGPT excels in medicine but falters in basic algebra*, ACA 2023 (Applications of Computer Algebra), Warsaw, Poland. DOI: 10.13140/RG.2.2.25600.20489

[3] E. Bagno, T. Dana-Picard and S. Reches (2024): *ChatGPT in Linear Algebra: Strides Forward, Steps to Go*, Open

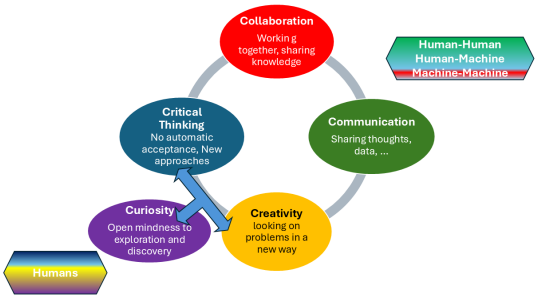


Figure 1.2: The 5 C's of 21st Century Education in a technology rich environment

Educational Studies 6 (1), pp. 20240031. https://doi.org/10.1515/edu-2024-0031
[4] N. Balacheff's (2022). *AI for the learning of mathematics*, in P. Richards, M.P. Vélez, S. Van Vaerenbergh (edts) Mathematics Education in the Age of Artificial Intelligence, Springer.
[5] F. Botana, T. Recio, M.P. Vélez (2024). *On Using GeoGebra and ChatGPT for Geometric Discovery*, Computers 13, 187. https://doi.org/10.3390/computers13080187
[6] Y. Chevallard (retrieved April 2025). *Pourquoi la transposition didactique?*, http://yves.chevallard.free.fr/spip/spip/\IMG/pdf/Pourquoi_la_transposition_didactique.pdf.
[7] T. Dana-Picard (2025). *Dynamic constructions of hyperbolisms of plane curves*, Electronic Journal of Technology in Mathematics 19(1). Online: https://ejmt.mathandtech.org/Contents/eJMT_v19n1p4.pdf
[8] T. Dana-Picard (2023). *Computer Assisted Proofs and Automated Methods in Mathematics Education*, in (P. Quaresma et al., edts), Proceedings of ThEdu '22 - 11th International Workshop on Theorem Proving Components for Educational Software, Electronic Proceedings in Theoretical Computer Science, 2-23. https://cgi.cse.unsw.edu.au/~eptcs/content.cgi?Thedu22.
[9] T. Dana-Picard and S. Hershkovitz (2023): *Pre-service teachers in a technology-rich environment: learning to do mathematics*, ICAS 2023 Conference: Innovative Design-Based Education Practices - The Power of Making, Seoul, Korea (online). DOI: https://doi.org/10.13140/RG.2.2.35547.95521
[10] T. Dana-Picard and Z. Kovács (2021): *Networking of technologies: a dialog between CAS and DGS*, The electronic Journal of Mathematics and Technology (eJMT) 15 (1), 43-59, 2021.

1.9 Automated methods applied for the exploration of singularities of some curves

Thierry Dana-Picard and Daniel Tsirkin
Jerusalem College of Technology, Israel

In memoriam Josef Böhm, a good friend dedicated to our community

We explore singularities of curves defined by geometric constructions using automated methods. A central feature of the work consists in networking between different kinds of software in order to use their respective strengths (dynamic geometry, strong algebraic computations, etc.). The activities have been proposed to in-service teachers learning towards an advanced degree.

1.10 Evaluation of the difficulty of a geometric statement: comparing ChatGPT and GeoGebra Discovery

Piedad Tolmos
Juan Carlos University, Spain

Our communication will present some initial results from an experience that we are developing, comparing the "complexity" measure assigned by GeoGebra Discovery's ShowProof command to a variety of well-known, elementary geometric statements, and the performance (i.e. correctness, clarity, and level of detail in the answer) of ChatGPT when asked about the same statements. Let us recall that the ShowProof command algorithmically outputs a proof by contradiction of a given geometric statement, expressing 1 as a combination of the hypotheses and the negation of the thesis. And ranks the "interest" or "difficulty" of the statement by computing the highest degree of the polynomials required to describe such contradiction. Measuring the interest of the output of automated reasoning tools is a classical challenge, but we think that the rank computed by the ShowProof command could be the first algorithmic approach towards establishing such measure

in the context of geometric statements, although yet requiring a careful experimental work, such as the one we are initiating now, regarding its practical performance..

1.11 Two methods for proving "Japanese Theorem II" using Maxima and KeTCindy: An Application of the MNR Method

Setsuo Takato
KeTCindy Center, Japan

Many of the plane geometry problems that appear in Wasan (Japanese Mathematics) are beautiful to look at but difficult to solve using computer algebra. In particular, triangular problems involve simultaneous equations with irrational expressions, which are extremely difficult to solve using normal methods. The author therefore devised a method to express the quantities of a triangle using $m = \tan\frac{B}{2}, n = \tan\frac{C}{2}$ and the radius of the inscribed circle r, which he named the MNR method. The author developed the Maxima MNR library and confirmed that it can solve various problems. It is possible to solve even more problems with techniques using quarter angles $M = \tan\frac{B}{4}, N = \tan\frac{C}{4}$.

1.12 Creating Stand-Alone Workspaces for Student Explorations with Maple™

William C. Bauldry
Appalachian State University, USA

We will investigate creating stand-alone workspaces based on the pedagogic principle of *Action-Consequence-Reflection* (ACR) [3]. The interactive workbooks we design may be accessed and used on the internet. Maple[1] is the main software tool we use to build the student exploration documents. We take advantage of the *Maple Cloud* for student web access.

Keywords: Action-Consequnce-Reflection Workspace, Stand-Alone Interactive Maple Document, Web-Based Maple Document

References

[1] W. Bauldry. "Microworlds with Maple for Investigating Complex Analysis." Joint Math. Meetings, San Antonio, 2015.

[2] W. Ellis. "Using Inquiry Questions and Action/Consequence Documents to Improve Student Understanding." MSRI - Mathematical Circles and Olympiads, 2004.

[3] W. Ellis and W. Bauldry. "Using and Creating *A-C-R* Documents for Mathematics Instruction with Computer Algebra." 15th ACA, Montreal, 2009.

[4] E. Marland, G. Rhoads, M. Bossé, J. Sanqui, and W. Bauldry. "Q^2: A Measure of Linearity," Electronic J. of Math. & Tech. Vol 14, No. 3 (Oct 2020). Available at: `https://ejmt.mathandtech.org/Contents/eJMT_v14n3n2.pdf`

[5] J. Post, T. Howell, K. Palmer, W. Bauldry, and M. Bossé. "Graphing the Remainder." Maple Transactions, Vol. 3, No. 1 (2023). Available at: `https://doi.org/10.5206/mt.v3i1.14322`

[6] J. Post, K. Palmer, W. Bauldry, and M. Bossé. "Getting Around to Rounding." MathAMATYC Educator, Fall 2023, Vol. 15, No. 1.

[1] Maple is a trademark of Waterloo Maple Inc.

1.13 Utilization of Algebrite in KeTLTS

Yasuyuki Kubo
Yuge KOSEN, Japan

This paper reports on the integration of algebrite, an online computer algebra system (CAS), into KeTLTS[2], a system developed by S. Takato using KeTCindyJS. Through this integration, we constructed a set of instructional materials that allow KeTLTS users to evaluate the validity of their answers before submission.

[2] https://s-takato.github.io/ketcindyorg/indexj.html

SPECIAL SESSION 2

Computer Algebra Software in the Life Sciences (CASinLife)

It is well-known that to answer a question, one must first state and formulate it properly. Many questions, from the effect of a drug on cancer cells to the spread of an epidemic, require mathematical modeling. Every project in the life sciences involves chemical materials, cells, or animals, with the ultimate goal of understanding how changes in the quantity of one element affect the others. While some questions can be addressed using basic methods, most require more sophisticated techniques. For instance, when measuring all relevant quantities is impossible, one encounters the issue of identifiability: is it possible to estimate the model's parameters using data from only the observable variables?

Computer Algebra, as the name suggests, is the field focused on developing algorithms for symbolic computations involving variables and parameters. While life scientists have a wealth of mathematically interesting questions, computer algebra researchers possess a wealth of algorithms and methods capable of addressing complex problems. Our session aims to bring these two groups together and facilitate the matching of questions with solutions. In addition to speakers from previous editions of CASinLife, who will report on collaborations sparked earlier, we are also seeking new participants with fresh challenges and ideas to join our ongoing journey of discovery.

This will be the fourth edition of CASinLife. The first three editions were held as special sessions of ACA 2022 (in Turkey), ACA 2023 (in Poland), and ICMS 2024 (in the UK). Topics of interests include, but are not limited to the following:

- Mathematical modelling for biological/chemical/ecological questions
- Chemical reaction network theory
- Combinatorial optimizations and machine learning tools for mathematical biology
- Cylindrical algebraic decomposition
- Quantifier elimination theory
- Computer algebra packages for real algebraic geometry
- Parameter identifiability analysis -Phylogenetics

Session organizers

- AmirHosein Sadghimanesh (Coventry University, UK)
- Andrzej Mizera (University of Warsaw, Poland)

2.1 Graph Neural Network-Based Reinforcement Learning for Controlling Biological Networks - the GATTACA framework

Andrzej Mizera
University of Warsaw and IDEAS Research Institute, Poland

Cellular reprogramming, the artificial transformation of one cell type into another, has been attracting increasing research attention due to its therapeutic potential for complex diseases. However, identifying effective reprogramming strategies through traditional wet-lab experiments is time-consuming and costly.

In this talk, we explore the use of deep reinforcement learning (DRL) to control Boolean network models of complex biological systems, such as gene regulatory and signalling pathway networks. We introduce the Graph-based Attractor-Target Control Algorithm (GATTACA), a framework designed to solve a novel, general target-control problem for BN models of biological networks under the asynchronous update mode, specifically in the context of cellular reprogramming. To facilitate scalability of GATTACA, we consider our previously introduced concept of a pseudo-attractor and we improve our procedure for effective identification of pseudo-attractor states. Then, we incorporate graph neural networks with graph convolution operations into the artificial neural network approximator of the DRL agent's action-value function to leverage the available knowledge on the structure of a biological system and to indirectly, yet effectively, encode the system's modelled dynamics into a latent representation.

Experiments on a number of large-scale, real-world biological networks from literature demonstrate the effectiveness and scalability of our approach.

2.2 Biological functions and functional modules originated in the structure of chemical reaction network

Atsushi Mochizuki
Institute for Life and Medical Sciences, Kyoto University, Japan

In living cells, chemical reactions are connected by sharing their products and substrates, and form a complex network system. Biological functions arise from the dynamics of chemical reaction networks, and are controlled by changes in the amount/activity of enzymes that catalyze reactions in the system. In this talk, I will introduce our recent theoretical approach to determine the behaviors of chemical reaction systems based solely on network topology. (1) We found that the qualitative response of chemical concentrations (and reaction fluxes) to changes in enzyme amount/activity can be determined from the network structure alone. (2) Non-zero responses are localized to finite ranges in a network, and each range is determined by a subnetwork called a "buffering structure". The buffering structure is defined by the following equation from local topology of a network $\chi := -(\#\text{ of chemicals}) + (\#\text{ of reactions}) - (\#\text{ of cycles}) + (\#\text{ of conserved quantities}) = 0$ where the index χ is analogous to the Euler characteristic. We proved that any perturbation of a reaction parameter inside a buffering structure only affects the concentrations and fluxes inside the buffering structure, and does not affect the concentrations nor fluxes outside. Finally, (3) buffering structures govern the bifurcation of the steady state of a reaction network. The bifurcation behaviors are localized to finite regions within a network, and these regions are again determined by buffering structures. These results imply that the buffering

structures are the origin of the modularity of biological functions derived from reaction networks. We applied this method to the cell cycle system and demonstrated that the control of different checkpoints is achieved by buffering structures.

2.3 Analyzing the dynamics and structure of biochemical reaction networks via network decomposition

Bryan Hernandez
University of the Philippines Diliman, Philippines

The complexity of biochemical reaction networks, characterized by their intricate structures and dynamic behaviors, presents considerable challenges in their analysis. To address these challenges, we apply network decomposition techniques to study the structural and dynamical properties of biochemical networks. In this approach, we decompose the network into independent subnetworks, where the stoichiometric matrices of the subnetworks can be directly summed to match the stoichiometric matrix of the entire network. This technique facilitates the computation of positive steady states, aiding in the description of long-term network behavior. We also observe a widespread property across many networks involving incidence-independent decomposition, where the incidence matrices of subnetworks can be directly summed to match the incidence matrix of the entire network. A key discovery is the phenomenon we term Finest Decomposition Coarsening (FDC), in which the finest independent decomposition (FID) is a coarsening of the finest incidence-independent decomposition (FIID). We characterize this property and find conditions under which these two types of decomposition coincide. Furthermore, we establish connections between these decompositions and the connected components of the network, known as linkage classes. This study provides a deeper understanding of the algebraic structure underlying biochemical reaction networks, advancing our ability to model and analyze their behavior.

2.4 Bayesian inference of interaction rates in a metabolite-bacteria network using time-series counts

Jack Jansma[1], Pietro Landi[1] and Cang Hui[1,2]
[1] Stellenbosch University, South Africa
[2] African Institute for Mathematical Sciences, South Africa

The human gut hosts a vast and diverse set of microbes that indirectly interact with each other through consuming and producing compounds, called metabolites. Disruptions in this network between gut microbes and their human host can contribute to the onset and progression of various disorders, including obesity, inflammatory bowel syndrome and Parkinson's disease. Understanding the intricate and dynamic interactions between microbes, metabolites and the host is essential for developing microbiota-targeted interventions to improve human health. To this end a precise mathematical framework is crucial to capturing the complex dynamics of the system.

Here, we develop a dynamic network model of coupled ordinary differential equations and present a computational workflow that integrates computer algebra with Bayesian inference for model identification. Our approach infers interaction rates—quantifying metabolite consumption

and production—from experimental time-series count data within a Bayesian framework, incorporating prior knowledge and uncertainty quantification. This workflow enables in silico predictions of system behaviour under perturbations and offers a robust method to integrate high-dimensional biological data with mechanistic models. By refining our understanding of gut microbial dynamics, this framework facilitates the assessment of microbiota-targeted therapeutic interventions.

Keywords: Gut microbiota, Bayesian inference, Ordinary differential equations

2.5 Reaction networks with (generalized) mass-action kinetics: Sign vector conditions for the existence of a unique general equilibrium

Marcus Aichmayr[1], Abhishek Deshpande[2], Stefan Müller[3] and Georg Regensburger[1]
[1] University of Kassel, Germany
[2] IIIT Hyderabad, India
[3] University of Vienna, Austria

We provide sufficient conditions for the existence of a unique equilibrium (in every compatibility class and for all rate constants), based on recent findings in [2]. Notably, our results apply to general equilibria, thereby extending previous results for special (toric or complex-balanced) equilibria, see e.g. [3]. Moreover, we consider both mass-action and generalized mass-action kinetics. We illustrate our methods by examples, using our SageMath package [1] available at `https://github.com/MarcusAichmayr/sign_vector_conditions`.

References

[1] M. S. Aichmayr, S. Müller, and G. Regensburger. A SageMath package for elementary and sign vectors with applications to chemical reaction networks. *In: Mathematical software—ICMS 2024*, Vol. 14749. Lecture Notes in Comput. Sci. Springer, Cham, 155–164, 2024.
[2] A. Deshpande and S. Müller. Existence of a unique solution to parametrized systems of generalized polynomial equations. 2024. url: `https://arxiv.org/abs/2409.11288`.
[3] S. Müller, J. Hofbauer, and G. Regensburger. On the bijectivity of families of exponential/generalized polynomial maps. *In: SIAM Journal on Applied Algebra and Geometry*, 3:412–438, 2019.

2.6 Symbolic bifurcation analysis of reaction networks with Python. Part I: Theory

Nicola Vassena
University of Leipzig, Germany

Computer algebra methods for analyzing reaction networks often rely on the assumption of mass-action kinetics, which transform the governing ODEs into polynomial systems amenable to techniques such as Gröbner basis computation and related algebraic tools. However, these methods face significant computational complexity, limiting their applicability to relatively small networks involving only a handful of species.

In contrast, building on recent theoretical advances, we present a symbolic approach designed to detect bifurcations in larger reaction networks (up to a few dozen species) equipped with a broad

class of "parameter-rich" kinetics. This class includes enzymatic kinetics such as Michaelis-Menten, ligand-binding kinetics like Hill functions, and generalized mass-action kinetics.

For a given network, the algorithm identifies all minimal autocatalytic subnetworks and fully characterizes the presence of bifurcations associated with zero eigenvalues, thus determining whether the network admits multistationarity. It also effectively detects oscillatory bifurcations arising from positive-feedback structures, capturing a significant class of possible oscillations.

The first talk (Vassena) will cover the theoretical foundations of this method, while the second (Golnik) will address its implementation in Python.

2.7 Graph-Theoretic Algorithms for Reducing Chemical Reaction Networks

Ovidiu Radulescu
University of Montpellier, France

Chemical reaction networks (CRNs) serve as models for complex biochemical processes occurring in cells and tissues. Studying these models is essential for understanding diseases, developing new therapies, controlling bioengineering processes, and gaining insights into fundamental aspects of living systems. However, many existing CRN models involve a large number of species and reactions, placing them beyond the reach of formal analysis methods. Additionally, parameter optimization for such models suffers from the curse of dimensionality. In previous work, we developed model reduction techniques that transform complex CRNs into simpler ones, with fewer species and reactions, making them more amenable to analysis and optimization. These approaches were based on tropical scaling and geometric singular perturbation theory. More recently, we introduced a graph-theoretical model reduction method based on the graph Laplacian. This method transforms CRNs algorithmically using graph rewriting on the species-reaction graph. In this presentation, I will show how model reduction via singular perturbations can also be formulated as a graph rewriting process and describe a general implementation of such algorithms. I will also discuss the application of these tools for generating hierarchies of models, where each model is derived from a more complex one through reduction. Such hierarchies can be used in AutoML strategies to select an appropriate model based on the available data and to use optimization results from simpler models to constrain and inform the optimization of more complex models as richer datasets become available.

2.8 Symbolic bifurcation analysis of reaction networks with Python. Part II: Implementation

Richard Goldnik
University of Leipzig, Germany

Computer algebra methods for analyzing reaction networks often rely on the assumption of mass-action kinetics, which transform the governing ODEs into polynomial systems amenable to techniques such as Gröbner basis computation and related algebraic tools. However, these methods face significant computational complexity, limiting their applicability to relatively small networks involving only a handful of species.

In contrast, building on recent theoretical advances, we present a symbolic approach designed to detect bifurcations in larger reaction networks (up to a few dozen species) equipped with a broad class of "parameter-rich" kinetics. This class includes enzymatic kinetics such as Michaelis-Menten, ligand-binding kinetics like Hill functions, and generalized mass-action kinetics.

For a given network, the algorithm identifies all minimal autocatalytic subnetworks and fully characterizes the presence of bifurcations associated with zero eigenvalues, thus determining whether the network admits multistationarity. It also effectively detects oscillatory bifurcations arising from positive-feedback structures, capturing a significant class of possible oscillations.

The first talk (Vassena) will cover the theoretical foundations of this method, while the second (Golnik) will address its implementation in Python.

2.9 New Results about Bricard's Flexible Octahedra

Robert H. Lewis[1], Mosavverul Hassan[2] and Evangelos Coutsias[3]
[1] Fordham University, NY, USA
[2] Vanderbilt University, TN, USA
[3] Stony Brook University, NY, USA

Biological functions such as signal transduction, enzymatic turnover, and allosteric regulation emerge as a consequence of protein conformational transitions (protein dynamics) across a complex energy landscape. Illuminating the mechanistic basis of protein function requires an understanding of why structures such as molecules can become flexible.

A polypeptide backbone can be modeled as a polygonal line whose edges and angles are fixed while some of the dihedral angles formed by successive triplets of edges vary freely, so that the structure is flexible. We model and analyze such a structure with a system of polynomial equations.

This subject has a long history.

- In 1812, Cauchy considered flexibility of three dimensional polyhedra (edges and faces), where each joint can pivot or hinge. He proved [2] that if the polyhedron is convex it must be rigid – i.e. cannot be flexible.
- In 1896 Bricard [1], following Cauchy, found three types of flexible non-convex octahedra, but the faces intercross, at least in 3-space.
- Following Bricard's ideas, Connelly (1978) found non-convex genuine flexible polyhedra [3] that really live in 3-space.

In spite of that success, key questions remained. Bricard asserted that a certain planar configuration of quadrilaterals can be flexible in the same way as the octahedra, since both systems satisfy the same set of polynomial equations:

$A_1 t^2 u^2 + B_1 t^2 + C_1 tu + D_1 u^2 + E_1,$
$A_2 u^2 v^2 + B_2 u^2 + C_2 uv + D_2 v^2 + E_2,$
$A_3 v^2 t^2 + B_3 v^2 + C_3 vt + D_3 t^2 + E_3$

Here the variables t, u, v represent angles and the coefficients are polynomials in the edges. The geometric structure is flexible if this system of polynomial equations has infinitely many solutions. In 2016 [4] we used computer algebra to show that the quadrilaterals have additional modes for flexibility. We did that by analyzing the Dixon resultant [5] of the system.

Another statement from Bricard [1], which has been called the Bricard conjecture, has remained unjustified until now:

Conjecture: The system of three equations above has infinitely many solutions iff t, u, and v satisfy both of these equations:

$a_1 t + b_1 u + c_1 v + d_1 tuv = 0,$
$a_2 tu + b_2 tv + c_2 uv + d_2 = 0,$
where the coefficients are polynomials in the edges. The "if" part here is easy, a simple exercise. The converse has never been proven.

Main Result: The converse is true for every known case of flexible structures. That includes the three types of flexible octahedra and every known case of the flexible planar quadrilaterals. The proof is with computer algebra, normalizing the 8×8 Dixon resultant, which contains polynomials in twelve variables with up to 100000 terms.

Secondary Result: As a biproduct of the main result, we have produced animations of Bricard's type three flexible octahedron. Apparently this has never been done before.

Keywords: flexible structures, octahedron, computer algebra

References

[1] Raoul Bicard. Mémoire sur la théorie de l'octaèdre articulé. *J. Math. Pures Appl.*, 3:113–150, 1897. English translation: `https://math.unm.edu/~vageli/papers/bricard$3_6$.pdf`.
[2] A. L. Cauchy. Sur les polygones et les polyhedres. *Second Memoire. Journal de l'École Polytechn.*, 9:8, 1813.
[3] R. Connelly. A counterexample to the rigidity conjecture for polyhedra. *Publications Mathématiques de l'I.H.É.S.*, 47:333–338, 1977.
[4] R. Lewis and E. Coutsias. Flexibility of Bricard's Linkages and Other Structures via Resultants and Computer Algebra. *Mathematics and Computers in Simulation*, 125:152–167, 2016.
[5] R. Lewis. Dixon-EDF: The Premier Method for Solution of Parametric Polynomial Systems. *In Applications of Computer Algebra 2015*, Springer Proc. in Math. & Stat., 198, 2017.

2.10 Learning treatment effects from multiple data

Sofia Triantafillou
University of Crete, Greece

Much of intelligence behaviour involves causal reasoning by predicting the effects of interventions. Causal inferences require experimental data, collected specifically for the estimation of a specific treatment effect. Such data however are expensive, difficult to collect and therefore scarce. Recent advances in data collection and sharing capacity have made vast amounts of observational data, such as electronic health record data, available to researchers. However, observational data are not necessarily appropriate for causal inference. Combining observational and experimental data can greatly improve causal predictions. In this talk, we discuss how causal models offer a language that connects different types of data and allows generalizing inferences across domains and populations.

2.11 Using ML tools to predict number of solutions of parametric system of polynomial equations with the help of CRNs

AmirHosein Sadeghimanesh

Coventry University, UK

Many questions in Chemical Reaction Network (CRN) theory can be framed as classifica- tion problems, such as the detection of multistationarity. In the age of AI, it is a common knowledge that there are plenty of machine learning (ML) algorithms capable of doing classi- fication tasks. These two sentences just made a clear motivation for using ML tools in CRN theory, and recently, in a work by the speaker and his colleagues, the first step in this direction has been taken. They introduced a new representation for CRN objects that helps us feed a CRN as an input to advanced ML algorithms. Multistationarity of a network mathemati- cally is the study of number of (positive) real solutions to a parametric system of polynomial equations describing the steady states of the network. This success together with Hungarian Lemma that states any given parametric polynomial system satisfying a technical condition can be associated to steady states of a CRN, triggers yet another idea. It is known that the deterministic symbolic algorithms to study the number of real solutions of parametric system of polynomial equations such as cylindrical algebraic decomposition are doubly exponential and so not practical for large size systems. Thus, we propose to use a new approach, convert- ing the system of equations to a CRN and then using the newly developed ML tools to predict the number of real solutions of the system.

References

[1] S. Yao, A. Sadeghimanesh and M. England. Designing Machine Learning Tools to Characterize Multistationarity of Fully Open Reaction Networks. 2024. https://arxiv.org/abs/2407.01760

[2] G. Craciun, M. D. Johnston, G. Szederkényi, E. Tonello, J. Tóth and P. Y. Yu. Realizations of kinetic differential equations. *Mathematical Biosciences and Engineering*, 12:6931–6945, 2020. https://doi.org/10.1016/j.amc.2013.01.027

SPECIAL SESSION 3

Computer algebra in group theory and representation theory

Groups are among the most fundamental objects of study in algebra. They appear naturally in the study of symmetries, but their nature is quite abstract. Representation theory allows us to study such abstract structures with the use of tools from linear algebra. For the study of concrete examples, computer algebra is extremely useful and many computer packages have been developed for this reason (including, but not limited to, GAP, Magma, Maple, SageMath). Moreover, there are families of finite groups, such as the sporadic simple groups or the exceptional complex reflection groups, for which most theoretical results have computational proofs. Finally, there are many discussions nowadays about the possibility of obtaining proofs to major open conjectures, as well as new theorems, with the use of computers. The session "Computer algebra in group theory and representation theory" will aim to cover all the topics mentioned above, with talks from researchers in group or representation theory who use or develop computer algebra tools.

Session organizers

- Maria Chlouveraki (National and Kapodistrian University of Athens, Greece)
- Ilias Andreou (National and Kapodistrian University of Athens, Greece)

3.1 The representations of the Brauer-Chen algebra associated to the exceptional complex reflection groups

Ilias Andreou
National and Kapodistrian University of Athens, Greece

In 1937, Richard Brauer extended Schur–Weyl duality to the case of the orthogonal group of transformations of a complex vector space by introducing its corresponding dual algebra, a natural extension of the group algebra of the symmetric group. Since then, the Brauer algebra has found connections outside the context of Schur–Weyl duality and has widely been generalized to larger classes of complex reflection groups. In this talk we study the generalization by Chen for all complex reflection groups and describe how we used GAP programming to obtain explicit results for the cases of exceptional complex reflection groups.

3.2 Coxeter groups via Cartan matrices

Maria Chatzikyriakou
National and Kapodistrian University of Athens, Greece

In this talk, based on my master thesis, we will see how we can study Coxeter groups with the use of Cartan matrices. Cartan matrices constitute a family of matrices with specific properties. We will discuss Matsumoto's theorem, as well as the cancellation law, both very important for Coxeter groups. Moreover, we will present the classification of finite Coxeter groups with the use of Dynkin diagrams. We will define root systems and use them to describe the generators of a Coxeter group. Finally, we will look at the longest element and its properties.

3.3 Blocks and Schur elements for Hecke algebras of exceptional complex reflection groups

Maria Chlouveraki
National and Kapodistrian University of Athens, Greece

Complex reflection groups are finite groups generated by (pseudo)reflections. They are products of irreducible complex reflection groups, which can either belong to the infinite series $G(de, e, n)$ or to the 34 exceptional groups $G_4, G_5, \ldots, G_{37}$. Most results obtained with the use of algebraic combinatorics for the former are obtained with the use of computer algebra for the latter. In this talk, we will give an overview of our results on the modular representation theory of Hecke algebras associated with exceptional complex reflections obtained computationally: from the description of blocks and Schur elements to the verification of old and new conjectures.

3.4 Decomposition of affine crystals in levels 1 and 2

Benedek Dombos
Université de Genève, Switzerland

Affine crystals in type A can be regarded as infinite ranked posets whose rankgenerating functions are classical infinite products (e.g. the Rogers–Ramanujan products appear in rank 1, level 3). I will describe two purely combinatorial decompositions of these crystals, yielding new infinite-sum formulas at levels 1 and 2, where the major index statistic naturally emerges. This is joint work with Jihyeug Jang.

3.5 The exotic nilCoxeter algebra for $G(m, m, 3)$

Daniel Juteau
Université de Picardie Jules Verne, France

Ben Elias introduced a q-deformation of the Cartan matrix of affine type A_{n-1}, which plays a role in the quantum geometric Satake equivalence. When q is specialized to a $2m$-th root of unity, the reflection representation factors through the complex reflection group $G(m, m, n)$. I will report on joint work with Ben Elias and Ben Young about the corresponding exotic nilCoxeter algebra, which is generated by q-deformed divided difference operators; this new algebra has surprising features. A classic result of Demazure, for Weyl groups, states that the polynomial ring of the reflection representation is a Frobenius extension over its subring of invariant polynomials, and describes how the Frobenius trace can be constructed within the nilCoxeter algebra. We study the analogous Frobenius extension for $G(m, m, n)$, and identify the Frobenius trace within the exotic nilCoxeter algebra for $G(m, m, 3)$.

3.6 Matroids

Angeliki Metallinou
National and Kapodistrian University of Athens, Greece

This talk offers a brief introduction to the theory of matroids, a combinatorial framework that generalizes the notion of linear independence beyond vector spaces. We will explore key definitions, fundamental examples, and important properties that make matroids a unifying structure across algebra, graph theory, and optimization. Special emphasis will be placed on the representability of matroids. The presentation is based on a master's thesis.

3.7 Steadied quotients of KLR algebras

Dinushi Munasinghe
National and Kapodistrian University of Athens, Greece

We give a brief overview of KLR algebras as diagrammatic presentations of blocks of cyclotomic quotients of Hecke algebras via Brundan and Kleshchev, and then discuss steadied quotients, a generalization of cyclotomic quotients introduced by Webster which we have recently shown to be low-dimensional representatives of Morita equivalence classes of Ariki–Koike blocks, as established by Scopes, Chuang–Kessar, Chuang–Rouquier, Evseev–Kleshchev, Webster, and others.

3.8 Reflection Groups in the Light of Formal Concept Analysis

Götz Pfeiffer
University of Galway, Ireland

Formal Concept Analysis (FCA) is a branch of applied lattice theory, concerned with the study of concept hierarchies derived from collections of objects and their attributes. Introduced by R. Wille in the 1980s, FCA now has found applications in machine learning and related fields. An application of FCA to hyperplane arrangements yields a new Galois connection on the (conjugacy classes of) parabolic subgroups of a finite reflection group. Combined with methods from Serre's recent work on involution centralizers, we obtain a refinement of Howlett's description of the normalizers of parabolic subgroups of a finite Coxeter group. This is joint work with G. Roehrle and J.M. Douglass.

3.9 The generalized Springer correspondence for disconnected reductive groups

Kostas Psaromiligkos
Université Clermont Auvergne, France

The generalized Springer correspondence provides a canonical partition of simple G-equivariant perverse sheaves on the nilpotent cone of a reductive group G into disjoint subsets known as induction series. Each series corresponds bijectively to the set of irreducible representations of a Weyl group. In this talk, I will discuss how to extend the correspondence to the setting where G is a disconnected complex reductive group and representations/sheaves over a field of arbitrary characteristic. I'll also present illustrative examples and computations, with the help of the CHEVIE package for organizing the relevant data. This is joint work with Simon Riche.

3.10 Toric ideals of graphs minimally generated by a Gröbner basis

Christos Tatakis
University of Western Macedonia, Greece

The problem of describing families of ideals minimally generated by either one or all of its Gröbner bases is a central topic in commutative algebra. This work tackles this problem in the context of toric ideals of graphs. We call a graph G an MG-graph if its toric ideal I_G is minimally generated by a Gröbner basis, while we say that G is an UMG-graph if every reduced Gröbner basis of I_G is a minimal generating set.

We prove that G is an UMG-graph if and only if I_G is a generalized robust ideal, i.e., ideal whose universal Gröbner basis and universal Markov basis coincide. We observe that the class of MG-graphs is not closed under taking subgraphs, and we prove that it is hereditary (i.e., closed under taking induced subgraphs). Also, we describe two families of bipartite MG-graphs: ring graphs and graphs whose induced cycles have the same length. The latter extends a result of Ohsugi and Hibi, which corresponds to graphs whose induced cycles have all length 4.

While working on this project, we have been making intensive and constant use of the software SageMath to generate examples and support conjectures. We also used the software SageMath for computing the whole Gröbner fan of the corresponding toric ideal, and thus we can only handle small examples in a reasonable amount of time. We have used the above computations together with the Nauty library to check that the only bipartite graph with ≤ 8 vertices that is not an MG-graph is the cube graph (the 1-skeleton of the 3-dimensional cube).

This is joint work with Ignacio García-Marco and Irene Márquez-Corbella.

SPECIAL SESSION 4

Computational Differential and Difference Algebra and Their Applications

Objectives

Algebraic differential and difference equations and systems of such equations arise in many areas of mathematics and in a wide range of subject areas including physics, biology, chemistry, economics, and engineering. Differential and difference computer algebra concerns the study of systems of differential and difference equations in a constructive way that extends methods and algorithms of commutative algebra and algebraic geometry. The main goal of the session is to discuss recent developments in computational methods of differential and difference algebra, as well as to explore new ideas and approaches oriented toward various applications of these methods.

Topics of the session include, but are not limited to

- Systems of Differential, Difference and Difference-Differential Algebraic Equations
- Differential and Difference Gröbner (Standard) and Involutive Bases
- Differential and Difference Characteristic Sets
- Triangular Decompositions of Differential and Difference Systems
- Differential and Difference Elimination
- Algorithmic Generation of Finite Difference Approximations to PDEs
- Consistency and Stability Analysis of Finite Difference Approximations
- Dimension Characteristics of Differential and Difference Algebraic Structures
- Difference Equations over Finite Fields and Their Applications
- Software Packages for Differential and Difference Algebra
- Applications of Differential and Difference Algebra in the Sciences

Session organizers

- Roberto La Scala (University of Bari Aldo Moro, Italy)
- Alexander Levin (The Catholic University of America, USA)
- Daniel Robertz (RWTH Aachen University, Germany)

4.1 Gröbner-type Bases with Respect to the Effective Order and Bivariate Dimension Polynomials of Difference Modules

Alexander Levin and Joseph Baranoski
The Catholic University of America, Washington, DC, USA

We introduce Gröbner-type bases in free difference modules that are associated with a reduction respecting the effective order of module elements. We prove some properties of such bases and present a Buchberger-type algorithm for their computation. The obtained results allows us to give a method of computation of a bivariate dimension polynomial of a finitely generated difference module. (The existence theorem for such a dimension polynomial was proved in [1], but that paper does not give a method of its computation.) We consider invariants of the bivariate difference dimension polynomials and show how they can be applied to the isomorphism problem for difference modules and to the equivalence problem for systems of algebraic difference equations. We also present a generalization of the results on multivariate difference dimension polynomials obtained in [2].

References

[1] A. Levin. Reduction with Respect to the Effective Order and a New Type of Dimension Polynomials of Difference Modules. *Proceedings of the 2022 International Symposium on Symbolic and Algebraic Computation (ISSAC '22)*, ACM, New York, 55–62.

[2] A. B. Levin. Computation of the Strength of Systems of Difference Equations via Generalized Gröbner Bases. *Gröbner Bases in Symbolic Analysis*, Walter de Gruyter, 2007, 43–73.

4.2 Integrability and Linearizability of a Family of Three-Dimensional Polynomial Systems

Bo Huang[1], Ivan Mastev[2] and Valery Romanovski[2]
[1] Beihang University, China
[2] University of Maribor, Slovenia

We investigate the local integrability and linearizability of a family of three-dimensional polynomial systems with the matrix of the linear approximation having the eigenvalues $1, \zeta, \zeta^2$, where ζ is a primitive cubic root of unity. We establish a criterion for the convergence of the Poincaré–Dulac normal form of the systems and examine the relationship between the normal form and integrability. Additionally, we introduce an efficient algorithm to determine the necessary conditions for the integrability of the systems. This algorithm is then applied to a quadratic subfamily of the systems to analyze its integrability and linearizability. Our findings offer insights into the integrability properties of three-dimensional polynomial systems.

References

[1] B. Huang; I. Mastev; V. Romanovski. Integrability and Linearizability of a Family of Three-Dimensional Polynomial Systems. *Journal of Systems Science and Complexity*. To appear.

[2] J. Llibre; C. Pantazi; S. Walcher First integrals of local analytic differential systems. *Bulletin des Sciences Mathématiques*, 136 (2012), 342–356.

4.3 Subresultants of Several Ore Polynomials

Jiaqi Meng and Jing Yang
Guangxi Minzu University, China

Subresultant theory is a fundamental tool in computer algebra and algebraic geometry, and its extension to several commutative polynomials has been a significant development in recent years. In this paper, we generalize the theory of subresultants to the setting of several Ore polynomials. Our contributions are as follows:

1. We introduce a novel definition of subresultants for several Ore polynomials, expressed explicitly in terms of their coefficients.
2. We demonstrate the utility of this definition by employing it to compute the parametric greatest common right divisor (GCRD) of several Ore polynomials.
3. We provide three equivalent expressions of the proposed definition, which are formulated in terms of the solutions of Ore polynomials.

References

[1] H. Hong; J. Yang. Subresultant of several univariate polynomials *Preprint.* arXiv: 2112.15370, 2021.
[2] H. Hong Ore subresultant coefficients in solutions. *Applicable Algebra in Engineering, Communication and Computing*, 12 (2001), 421–428.
[3] Z. Li A subresultant theory for Ore polynomials with applications. *Proceedings of the 1998 international symposium on Symbolic and algebraic computation (ISSAC 1998)*, 132–139. Editors: V. Weispfenning and B. Trager.

4.4 Iterated strongly normal extensions and nonlinear differential equations

V. Ravi Srinivasan and Partha Kumbhakar
IISER Mohali, India

In this talk, I will sketch various results describing the structure of differential subfields of iterated strongly normal extensions. These results will then be used to study differential algebraic dependence of generic solutions in iterated strongly normal extensions of nonlinear differential equations. Our results along with the work [1], immediately proves that the Lotka-Volterra system

$$\begin{cases} y_1' = \alpha y_1 + \beta y_1 y_2 \\ y_2' = \gamma y_2 + \delta y_1 y_2 \end{cases}$$

where $\alpha, \beta, \gamma, \delta \in \mathbb{C} \setminus 0$, has a generic solution in an iterated strongly normal extension E of $\mathbb{C}$ if and only if $\alpha = \gamma$, which in turn holds if and only if the generic solution is in an elementary extension of $\mathbb{C}$ and that the Poizat differential equation $y'' = y' f(y)$, where $f \in \mathbb{C}(y)$, has no generic solution in an iterated strongly normal extension of $\mathbb{C}$.

References

[1] Christine Eagles and Léo Jimenex. Internality of autonomous algebraic differential equations. *arXiv*:2409.01863v1.

4.5 Stream cipher over Finite Fields: A Difference Algebra Approach

Roberto La Scala
Università degli Studi di Bari, Italy

Many stream ciphers of real practical interest, such as Trivium and Bluetooth's E0, can be modeled as systems of difference equations with coefficients and solutions in a finite field. Alongside this system of equations, one also needs a polynomial that enables the calculation of the keystream elements from the cipher register. This register can indeed be considered the state whose evolution is governed by the system of explicit ordinary difference equations. Such a system ensures that each state is uniquely determined by the initial state, which effectively serves as the cipher's key. We will refer to this class of stream ciphers as "difference ciphers".

Using the formalism of Difference Algebra, it is possible to define some relevant properties of stream ciphers, in particular their invertibility and periodicity. These properties are introduced in terms of fundamental functions associated with the difference system, such as the "state transition endomorphism" and its corresponding "state transition map". Additionally, it is possible to precisely define an algebraic attack on the cipher based on the knowledge of a certain number of keystream elements. The property of a cipher being invertible also allows for the optimization of such an attack, which can drastically reduce the security of the cryptosystem. Indeed, assuming invertibility, it is sufficient to calculate any internal state, such as the one from which the keystream begins, to know the initial state that contains the key. To determine if a difference cipher is invertible, one can use the calculation of a Gröbner basis of an ideal associated with the state transition endomorphism. This computation also yields the inverse difference system, enabling the reversal of the cipher's clock progression.

Another critical property for the security of such stream ciphers is the non-linearity of the difference equations and/or the keystream polynomial. Indeed, it is well known that a system of LFSRs, which corresponds to the fully linear case, can be attacked in polynomial time. In the presence of non-linear equations in the system, however, an algebraic attack corresponds to solving a system of non-linear polynomial equations over a finite field, the resolution of which is generally an NP-complete problem. Using the notion of difference cipher, we can analyze the various systems of polynomial equations corresponding to different types of algebraic attacks and understand why they are complex to solve.

Finally, to illustrate these concepts and the corresponding cryptanalytic techniques, we consider the stream ciphers Trivium and E0. These ciphers have been the subject of recent attacks in [1], [2], [3].

References

[1] La Scala, Roberto; Pintore, Federico; Tiwari, Sharwan K.; Visconti, Andrea. A multistep strategy for polynomial system solving over finite fields and a new algebraic attack on the stream cipher Trivium. *Finite Fields Appl.*, 98 (2024), Paper No. 102452, 1–33.

[2] La Scala, Roberto; Polese, Sergio; Tiwari, Sharwan K.; Visconti, Andrea. An algebraic attack to the Bluetooth stream cipher E0. *Finite Fields Appl.*, 84 (2022), Paper No. 102102, 1–29.

[3] La Scala, Roberto; Tiwari, Sharwan K. Stream/block ciphers, difference equations and algebraic attacks. *J. Symbolic Comput.*, 109 (2022), 177–198.

4.6 A Reduce package for Differential Operators in Mathematical Physics and Theoretical Physics

Raffaele Vitolo
University of Salento, Italy

The mathematical subject 'Geometry of Differential Equations', although not mainstream, covers many topics which have significant overlap with several other branches of Mathematics, like symmetries and conservation laws of ODEs and PDEs, Hamiltonian or symplectic formalism for ODEs and PDEs, integrability. See the books [1] and [5] for an overview. The CDE package was developed in Reduce with the purpose of providing a tool for computations in the above field [4]. This package has already been used in a number of papers (*e.g.* [2], [3] and [6] to [8]).

Recent developments of the capabilities of CDE go in the direction of computing with differential operators. We will show how newly added software can be used for typical computations related with the search of Lax pairs (joint work with R. La Scala, Un. of Bari, Italy), or can provide an environment for calculations in Supersymmetric Quantum Mechanics (joint work with L. Miranda and F. Toppan CBPF – Rio De Janeiro, Brazil).

References

[1] A. V. Bocharov, V. N. Chetverikov, S. V. Duzhin, N. G. Khor′kova, I. S. Krasil′shchik, A. V. Samokhin, Yu. N. Torkhov, A. M. Verbovetsky, and A. M. Vinogradov. *Symmetries and Conservation Laws for Differential Equations of Mathematical Physics.* Monograph. Amer. Math. Soc., 1999. I. S. Krasil′shchik and A. M. Vinogradov editors.

[2] M. Casati, P. Lorenzoni, D. Valeri, and R. Vitolo. Weakly nonlocal Poisson brackets: tools, examples, computations. *Computer Physics Communications*, 274:108284, 2022, DOI: https://doi.org/10.1016/j.cpc.2022.108284, arXiv: https://arxiv.org/abs/2101.06467.

[3] M. Casati, P. Lorenzoni, and R. Vitolo. Three computational approaches to weakly nonlocal poisson brackets. *Stud. Appl. Math.*, 144(4):412–448, 2020, DOI: 10.1111/sapm.12302, arXiv: https://arxiv.org/abs/1903.08204.

[4] J. Krasil′shchik, A. Verbovetsky, and R. Vitolo. *The symbolic computation of integrability structures for partial differential equations.* Texts and Monographs in Symbolic Computation. Springer, 2018. ISBN 978-3-319-71654-1; see http://gdeq.org/Symbolic_Book for downloading program files that are discussed in the book.

[5] P.J. Olver. *Applications of Lie Groups to Differential Equations.* Springer-Verlag, 2nd edition, 1993.

[6] S. Opanasenko and R. Vitolo. Bi-Hamiltonian structures of wdvv type. *Proc. R. Soc. Lond. Ser. A Math. Phys. Eng. Sci.*, 480:20240249, 2024, DOI: https://doi.org/10.1098/rspa.2024.0249 arXiv: https://arxiv.org/abs/2407.17189.

[7] J. Vašíček and R. Vitolo. WDVV equations and invariant bi-Hamiltonian formalism. *J. of High Energy Physics*, 129, 2021, arXiv: https://arxiv.org/abs/2104.13206. Calculations in GitHub: https://github.com/Jakub-Vasicek/WDVV-computations.

[8] R. Vitolo. Computing with Hamiltonian operators. *Comput. Phys. Comm.*, 244:228–245, 2019, arXiv: https://arxiv.org/abs/1808.03902.

4.7 Symbolic integration on a planar differential foliation

Thierry Combot
University of Bourgogne, France

In this presentation, we will study the differential algebraic properties of integrals of the form $\int G(x, y(x, h))dx$ where y is a family of solutions of differential equations.

Consider a differential equation $y' = F(x, y)$ with F rational. This equation defines a foliation of the plane $\mathcal{F}$, and we consider the integral $\int_{\mathcal{F}} G(x, y(x))dx$ along the leaves of $\mathcal{F}$, with G rational. Alternatively, we can write $I(x, h) = \int G(x, y(x, h))dx$ where $y(x, h)$ is a family of solutions of $y' = F(x, y)$. if $\mathcal{F}$ is an algebraic foliation, such integral is D-finite and is always differentially algebraic in h. Oppositely, let us assume that $y' = F(x, y)$ has no rational first integral. We will prove that if $I(x, h)$ is differentially algebraic, then, up to parametrization change in h, $I(x, h)$ satisfies a differential equation of the form $LI = (\partial y(x, h))^{\ell} H(x, y(x, h))$ where $L \in \mathbb{C}[\partial_h]$ has constant coefficients. The possible operators L depends on the existence of an integrating factor for $y' = F(x, y)$ and its algebraic nature. We will present an efficient algorithm to find such minimal integrating factor. We will then present an algorithm to find a differential relation up to some given bound on the order of L and degree of H. In the particular case of the foliations $y = \ln x + h$ et $\ln y = \alpha \ln x + h$, we have a complete algorithm to decide if integrals are differential algebraic, and this leads to explicit formulas in terms of special functions Ei, Li, Φ. This allows to study the differential transcendence of the flow of a differential equation in the plane. If possible, we will present how this generalizes in higher dimension.

References

[1] Thierry Combot. Symbolic integration on a planar differential foliation, 21 Jun 2023. `https://arxiv.org/abs/2306.12573`.

4.8 Affirmative answer to the Question of Leroy and Matczuk on injectivity of endomorphisms of semiprime left Noetherian rings with large images

V. V. Bavula
University of Sheffield, UK

The class of semiprime left Goldie rings is a huge class of rings that contains many large subclasses of rings – semiprime left Noetherian rings, semiprime rings with Krull dimension, rings of differential operators on affine algebraic varieties and universal enveloping algebras of finite dimensional Lie algebras to name a few. In 2013, the paper, 'Ring endomorphisms with large images,' *Glasg. Math. J.* **55** (2013), no. 2, 381–390, A. Leroy and J. Matczuk posed the following question [1]:

If a ring endomorphism of a semiprime left Noetherian ring has a large image, must it be injective?

The aim of the paper is to give an affirmative answer to the Question of Leroy and Matczuk and to prove the following more general results.

Theorem. (Dichotomy) *Each endomorphism of a semiprime left Goldie ring with large image is either a monomorphism or otherwise its kernel contains a regular element of the ring ($\Leftrightarrow$ its kernel is an essential left ideal of the ring). In general, both cases are non-empty.*

Theorem. *Every endomorphism with large image of a semiprime ring with Krull dimension is a monomorphism.*

Theorem. (Affirmative answer to the Question of Leroy and Matczuk) *Every endomorphism with large image of a semiprime left Noetherian ring is a monomorphism.*

References

[1] A. Leroy and J. Matczuk Ring endomorphisms with large images *Glasg. Math. J.*, 55, no. 2: 381–390, 2006.

SPECIAL SESSION 5

Computer algebra modeling in physics, classical and celestial mechanics, and engineering

The progressive impact of Computer Algebra Systems (CAS) in science-based disciplines is vividly noticeable. It is rare to encounter a scientific investigation immune from its beneficial influences. Within 30 years, the CAS has become an efficient tool for analyzing engineering and mathematical challenges. Symbolic capabilities of the CAS provide a forum to perform amazing calculations that practically are impossible otherwise. For instance, dynamic simulations of engineering issues are addressed, and mathematical conjectures are formulated and verified. Many problems in physics and mechanics are tackled by applying the perturbation theory, which implies that quite cumbersome symbolic calculations can be solved efficiently with the CAS.

The purpose of organizing this session is to bring together enthusiastic users of Computer Algebra Systems in science and engineering. Expected topics of presentations include (but are not limited to):

- symbolic and numerical methods for solving ODEs
- modeling and simulation in physics and engineering
- applications in classical and celestial mechanics
- perturbation theories

Session organizers

- Alexander Prokopenya (Institute of Information Technology, Warsaw University of Life Sciences – SGGW, Poland)
- Haiduke Sarafian (Professor Emeritus of Physics and John T. and Paige S. Smith Professor of Science Emeritus, The Pennsylvania State University, USA)

5.1 An Attempt to Create Teaching Materials for the Brachistochrone Curve Using Algebrite and KeTLTS

Setsuo Takato
KeTCindy Center, Magnolia Inc., Japan

KeTCindy/KeTCindyJS is a library for LaTeX and HTML that we have developed. It is based on the dynamical geometry system Cinderella. Using it, we have also created a learning data transfer system named KeTLTS. The brachistochrone curve is an interesting topic in mathematics and physics education, so we produced the HTML with KeTLTS.

5.2 Possible Orderings of Mode, Median, and Mean in Unimodal Distributions

Arkadiusz Orłowski
Instytut Informatyki Technicznej, WULS-SGGW, Poland

It is obvious that in symmetric and unimodal probability distribution functions (PDFs), the *mode*, *median*, and *mean* coincide. In asymmetric distributions, the typical ordering of these measures follows a predictable pattern: mode < median < mean (for right-skewed PDFs) or mean < median < mode (for left-skewed PDFs). This pattern is so entrenched that even in modern textbooks it is seldom, if ever, disputed.

This raises a natural and surprisingly deep question: *Are other orderings of mode, median, and mean possible?* In particular, are *all four* remaining orderings realizable? One can show that some such different orderings are indeed possible — e.g., by forming artificial mixtures of PDFs or adding a local peak to distort the density. However, such constructions usually lead to multimodal and highly irregular distributions, undermining their statistical relevance. While scattered examples in the literature [1] and [2] show that *some* alternative orderings may also arise even in unimodal PDFs, there has been *no systematic study* exploring the full set of six possible orderings under the unimodality constraint.

Here, we undertake such a study, leveraging the power of Computer Algebra Systems (CAS) and symbolic-numeric tools which allow us to explore complex nonlinear relationships between distribution parameters and the resulting positions of the mode, median, and mean. As a result we find examples of PDFs providing all six orderings. We compute and plot the corresponding PDFs to verify unimodality and to visually confirm the relative locations of the parameters. It shows that even basic statistical notions can exhibit unexpected structural richness, and that CASs provide a powerful framework for resolving such challenging questions. Possible applications in physics and engineering are also given.

Keywords: Mode, Median, Mean

References

[1] R. A. Groeneveld, Skewness for the Weibull Family. *Statistica Neerlandica* **volume** 40, 135–140 (1986).
[2] S. Basu, A. DasGupta, The Mean, Median, and Mode of Unimodal Distributions: A Characterization. *Theory of Probability & Its Applications* **volume** 41, 210–223 (1997).

5.3 Classification of Universal Decision Elements Using Computer Algebra Systems

Arkadiusz Orłowski
Instytut Informatyki Technicznej, WULS-SGGW, Poland

The concept of Universal Decision Elements (UDEs) emerged in the 1950s [1] and underwent further development in the 1960s-70s [2] and [3]. These early efforts, although insightful, were constrained by the limitations of contemporary hardware and lacked exhaustive formal analysis. Here, we revisit the problem from a modern perspective, leveraging the power of Computer Algebra Systems to perform a complete and verifiable classification of all possible UDEs within a clearly defined logical and functional framework.

We introduce a rigorous formalization of the UDE concept, define the precise criteria for their universality, and use symbolic computation to systematically analyze the entire space of candidate logical functions. The resulting classification reveals both known and previously unrecognized universal elements, providing a comprehensive map of the UDE landscape.

Finally, we propose a series of generalizations of the classical UDE framework, extending it to accommodate reversible computing and quantum information processing. By reframing UDEs in terms compatible with reversibility, we contribute to the rapidly evolving field of reversible and quantum computation, and suggest that long-overlooked and largely forgotten constructs from mid-20th-century logic design may acquire new relevance in the emerging paradigms of reversible logic synthesis and post-classical computation.

Keywords: Universal Decision Element

References

[1] B. Sobociński, On a universal decision element. *The Journal of Computing Systems* **volume** 1, 71–80 (1953).
[2] E. Foxley, Determination of the set of all four-variable formulae corresponding to universal decision elements using a logical computer. *Mathematical Logic Quarterly* **volume** 10, 302–314 (1964).
[3] J. C. Muzio, Partial universal decision elements. *Notre Dame Journal of Formal Logic* **volume** 15, 133–140 (1974).

5.4 Study of the secular perturbations in the three-planetary four-body problem with isotropically varying masses

Saltanat Bizhanova[1], Mukhtar Minglibayev[1,2] and Alexander Prokopenya[3]
[1] Al-Farabi Kazakh National University, Kazakhstan
[2] Fesenkov Astrophysical Institute Observatoriya, Kazakhstan
[3] Warsaw University of Life Sciences, Poland

Three-planetary four-body problem with variable masses is considered in a general case when the masses of the bodies vary isotropically at different rates. The problem is investigated in osculating elements of aperiodic motion on quasi-conic section [1], [2] and [3], using the equations of perturbed motion in the Lagrange form. The equation of the perturbed motion were averaged over the mean longitudes of the bodies in the absence of mean motion resonances and the differential equations describing the long-term evolution of the orbital parameters were obtained. Numerical calculations of the evolution of analogs of orbital elements of planets in an exoplanetary system

were performed using evolutionary equations in the Lagrange form and the Wolfram Mathematica computer algebra system.

Keywords: Four-body problem, Variable mass, Non-stationary exoplanetary systems, Aperiodic motion, Perturbations, Wolfram Mathematica

References

[1] M.Zh. Minglibayev, *Dynamics of Gravitating Bodies of Variable Masses and Sizes.* Lambert Academic Publ., Saarbrucken, 2012.

[2] M. Minglibayev, A. Prokopenya, G. Mayemerova, Zh. Imanova, Three-body problem with variable masses that change anisotropically at different rates. *Mathematics in Computer Science* **11**, 383–391 (2017).

[3] A. Prokopenya, M. Minglibayev, S. Shomshekova , Applications of computer algebra in the study of the two-planet problem of three bodies with variable masses. *Programming and Computer Software* **45**(2), 73–80 (2019).

5.5 Convergence order in trajectory estimation with piecewise Bézier cubics based on reduced data

Ryszard Kozera[1,2] and Magdalena Wilkołazka[3]
[1] Warsaw University of Life Sciences - SGGW, Poland
[2] The University of Western Australia, Australia
[3] The John Paul II Catholic University of Lublin, Poland

We discuss the problem of fitting reduced data $\mathcal{Q}_m = \{q_i\}_{i=1}^m$ in arbitrary Euclidean space $\mathbb{E}^n$. In our setting the interpolation knots $\{t_i\}_{i=0}^m$ (with $q_i = \gamma(t_i)$) are unknown and need to be compensated by certain $\hat{\mathcal{T}} = \{\hat{t}_i\}_{i=0}^m$ (see e.g. [1]). Various fitting schemes combined with some recipes for $\hat{\mathcal{T}}$ were studied e.g. in [1], [2] and [3] (for dense $\mathcal{Q}_m$) or [4] and [5] (for sparse $\mathcal{Q}_m$). In case of $\mathcal{Q}_m$ dense, the convergence rate (and its sharpness) for a selected interpolation scheme $\hat{\gamma}$ (based on $\mathcal{Q}_m$ and $\hat{\mathcal{T}}$) in approximating γ is a task to examine - see e.g. [2], [3] and [4]. We analyze the problem of partially fitting $\mathcal{Q}_m$ by merely interpolating $\hat{\mathcal{Q}}_m = \{q_0, q_3, q_6, \ldots, q_{m=3k}\}$ with piecewise cubic Bézier curve $\hat{\gamma}_B$ (see [6]). The other points serve only as control points. *A sharp quadratic order* in γ estimation by $\hat{\gamma} \circ \varphi$ (with $\varphi : [0, T] \to [0, \hat{T}]$) is proved. Numerical and symbolic computation in *Mathematica* is used to confirm the latter.

Keywords: Interpolation, Reduced Data, Convergence Orders and Sharpness

References

[1] B.I. Kvasov, *Methods of Shape Preserving Approximation.* World Scientific, Singapore, 2000.

[2] M.S. Floater, Chordal cubic spline interpolation is fourth-order accurate. *IMA Journal of Numerical Analysis* **26**, 25–33, (2005).

[3] R. Kozera; L. Noakes; M. Wilkołazka, Exponential parameterization to fit reduced data. *Applied Mathematics and Computation* **391**, 1–19, article no. 125645 (2021).

[4] R. Kozera; L. Noakes; A. Wiliński, Generic case of Leap-Frog Algorithm for optimal knots selection in fitting reduced data. In *Computational Sciences - ICCS 2021*, M. Paszyński et al. (eds.), 337–350. LNCS 12745, Cham, Springer, 2021.

[5] E. Kuznetsov; A. Yakimovich, The best parameterization for parametric interpolation. *Journal of Computational Applied Mathematics* **191**(2), 239–245, (2006).

[6] L. Piegl; W. Tiller, *The NURBS Book.* Springer-Verlag, Berlin Heidelberg, 1997.

5.6 Symbolic computations in studying the stability of nonlinear oscillations of the mathematical pendulum

Alexander Prokopenya
Warsaw University of Life Sciences – SGGW, Poland

The mathematical pendulum is a simple mechanical system with one degree of freedom and its motion is determined by the second order ordinary differential equation [1]. Its general solution may be written in terms of the Jacobi elliptic functions and describes a periodic motion of the pendulum in the domain $\phi \in [-a, a]$, where a is the amplitude of oscillations. From the other side, using the Poincare-Lindstedt method [2], one can construct this periodic solution in the form of power series in the amplitude a that is assumed to be small [3]. As the oscillation frequency depends on the amplitude, the periodic solution is unstable in Lyapunov sense. The main aim of this talk is to demonstrate the most important and useful algorithms for studying the stability of periodic solutions, considering the nonlinear oscillations of the mathematical pendulum as an example. Implementation of the corresponding algorithms involves quite cumbersome symbolic computation which may be performed efficiently with the aid of the computer algebra systems, for instance, Wolfram Mathematica.

Keywords: Nonlinear oscillations, Stability, Symbolic calculation, Wolfram Mathematica

References

[1] H. Goldstein, Ch.P. Poole, J.L. Safko, *Classical Mechanics.* Addison Wesley, New York, 2000.
[2] A.H. Nayfeh, *Introduction to Perturbation Techniques.* Wiley, New York, 1981.
[3] A. Prokopenya, Nonlinear oscillations of mathematical pendulum. In *Computer Algebra Systems in Teaching and Research, vol. XI, Mathematical Modelling and Differential Equations*, A. Prokopenya, A. Gil-Swiderska, M. Siluszyk (eds.), 119–132. Siedlce University of Natural Sciences and Humanities, Siedlce, 2022.

5.7 Secular perturbations in the four-body system with anisotropically varying masses

Moldir Saparova[1], Mukhtar Minglibayev[1,2] and Alexander Prokopenya[3]
[1] Al-Farabi Kazakh National University, Kazakhstan
[2] Fesenkov Astrophysical Institute Observatoriya, Kazakhstan
[3] Warsaw University of Life Sciences, Poland

We consider the classical problem of four bodies attracting each other according to Newton's law of universal gravitation. The masses of the bodies are assumed to vary anisotropically with different rates, which leads to the appearance of reactive forces. Since the differential equations of motion of the system are not integrable, the problem is studied in the framework of the perturbation theory methods, where quite cumbersome symbolic calculations are involved (see [1], [2] and [3]). An exact solution to the two-body problem with variable masses describing the aperiodic motion of the bodies along quasi-conical section is used as the first approximation. The equation of the perturbed motion are obtained in terms of the osculating orbital elements. Averaging these equations over the mean longitudes of the bodies in the absence of mean motion resonances, we derive the differential equations describing the long-term evolution of the orbital parameters. All relevant symbolic calculations are performed with the aid of the computer algebra system Wolfram Mathematica.

Keywords: Four-body problem, Variable mass, Evolutionary equations, Secular perturbations, Wolfram Mathematica

References

[1] M.Zh. Minglibayev, *Dynamics of Gravitating Bodies of Variable Masses and Sizes.* Lambert Academic Publ., Saarbrucken, 2012.
[2] M. Minglibayev, A. Prokopenya, G. Mayemerova, Zh. Imanova, Three-body problem with variable masses that change anisotropically at different rates. *Mathematics in Computer Science* **11**, 383–391 (2017).
[3] A. Prokopenya, M. Minglibayev, M. Saparova , Symbolic calculations in the study of secular perturbations in the many-body problem with variable masses. *Programming and Computer Software* **51**(1), 32–40 (2025).

5.8 Kinematics of a point-like charge particle in nontrivial non-homogeneous electric fields of charged washers

Haiduke Sarafian
Pennsylvania State University, USA

In this research-oriented passage, first, we explore the electric field of various charged commonly used circular washers. The scope of the study is extended by exploring non-common rectangular washers. Thirdly, by combining the circular and rectangular curved washers, an unusual washer is designed to explore its electric field; see figures. The second exploration segment focuses on the kinematics of a point-like charged particle within the mentioned fields. The complicated mathematical issues of the second and third mentioned cases are ironed out by applying a Computer Algebra System (CAS), namely, Mathematica [1], [2] and [3]. Taking advantage of the crafted numeric solutions of the changeling differential equations, various phase diagrams are constructed supporting the intuitively predicted outputs are just. All the used Mathematica codes are embedded, making the reproductions of the report reproducible.

Keywords: Electric Field, Non-common Curved Rectangular Washer, Computer Algebra System, Mathematica

References

[1] Mathematica 14.1 `http://Wolfram.com`
[2] Wolfram, S. (2003) The Mathematica Book. 5th Edition, Cambridge University Publications, Cambridge).
[3] Sarafian, H. (2024) American Journal of Computational Mathematics, 14, 240-247

5.9 Oscillation analysis of a bifilar pendulum with Mathematica

Haiduke Sarafian
Pennsylvania State University, USA

Utilizing a Computer Algebra System (CAS), namely Mathematica, the characteristics of a bifilar disk-shaped pendulum have been studied. By applying the Lagrangian methodology, the disk's motion equation is formulated. This is conducive to an ODE, as its numeric solution coincides with intuitive expectation. The period of the oscillations and tension in the strings are calculated and graphed.

Keywords: Bifilar Pendulum, Oscillation Period, ODE, Mathematica

References

[1] Mathematica 14.1 http://Wolfram.com
[2] Wolfram, S. (2003) The Mathematica Book. 5th Edition, Cambridge University Publications, Cambridge).
[3] Sarafian, H. (2024) American Journal of Computational Mathematics, 14, 240-247

5.10 An overview of averaging methods in Hamiltonian perturbation theory, using a CAS

José A. Vallejo
Universidad Nacional de Educación a Distancia, Spain

The Hamiltonian formalism is particularly well-suited for employing perturbation techniques. A widely used procedure involves transforming the system under consideration into its normal form [1], followed by the application of an averaging method to derive an approximate dynamics [2]. The computations in this latter stage can become quite cumbersome to perform manually, making it an ideal context to leverage the capabilities of a Computer Algebra System (CAS). In this talk, I will describe several examples illustrating the existence of stable closed orbits within seemingly chaotic systems, using these concepts and the free CAS Maxima [3] and [4].

Keywords: Normal forms, Averaging methods, Closed orbits

References

[1] M. Avendaño-Camacho, J. A. Vallejo, Yu. Vorobiev: A simple global representation for second-order normal forms of Hamiltonian systems relative to periodic flows. Journal of Physics A: Mathematical and Theoretical 2013 DOI: 10.1088/1751-8113/46/39/395201
[2] M. Avendaño-Camacho, J. A. Vallejo, Yu. Vorobiev: Higher order corrections to adiabatic invariants of generalized slow-fast Hamiltonian systems. Journal of Mathematical Physics 2013 DOI: 10.1063/1.4817863
[3] M. Avendaño-Camacho, J. A. Vallejo, Yu. Vorobiev: A perturbation theory approach to the stability of the Pais-Uhlenbeck oscillator. Journal of Mathematical Physics 2017 DOI: 10.1063/1.5000382
[4] M. Avendaño-Camacho, M. A. Manotas, J. A. Vallejo: Closed stable orbits in a strongly coupled resonant Wilberforce pendulum. Journal of Vibration and Control. 2022-04 DOI: 10.1177/1077546320986023

SPECIAL SESSION 6

Symbolic Linear Algebra and Its Applications

Symbolic Linear Algebra is now a mature subject at the heart of symbolic computation, with many important sub-disciplines and complementary aspects. Fundamentally, the field is concerned with computing with linear operators and matrices of mathematical entries, whether over an exact domain (such as the integers or a finite field), structured types (such as univariate or multivariate polynomials, with exact or approximate coefficients), or even more general fields and rings (such as differential operators). Enormous strides have been made in the development of algorithms and their realization in innovative software libraries and computer algebra systems. But even after six decades or more of theory and practice, progress is still being made in the efficiency and complexity, scope of matrix operations, diversity of underlying domains, and exploitation of matrix structure. Moreover, all advances have the potential to increase the ability for computer algebra systems to solve larger and more interesting problems and increase their field of application.

In this broad session, we will consider all aspects of the above, including:

- Algorithms for multivariate and parameterized matrices
- Structured linear algebra, e.g. for totally nonnegative matrices
- Sparse matrices and sparse domains
- Black-box and iterative matrix methods
- Complexity of linear algebra algorithms and problems
- Symbolic-numeric methods and stability analyses
- Matrices of differential and difference (Ore) polynomials
- Bohemian matrices, random matrices and experimental matrix algebra
- Implementation and libraries for symbolic linear algebra

We will be especially interested in the application of established and novel symbolic linear algebra techniques, software, and systems to real-world problems.

Session organizers

- Robert M. Corless (University of Western Ontario, London, Ontario, Canada)
- Mark Giesbrecht (Cheriton School of Computer Science, University of Waterloo, Waterloo, Ontario, Canada)

6.1 On the maximal spread of symmetric Bohemian matrices

Robert M. Corless
University of Western Ontario, Canada

Let A be a square matrix with entries in $\mathbb{R}$. The spread of A is defined as the maximum of the distances between the eigenvalues of A. Let $S_m[a, b]$ denote the set of all $m \times m$ symmetric matrices with entries in the real interval $[a, b]$ and let $S_m\{a, b\}$ be the subset of $S_m[a, b]$ of Bohemian matrices with population from only the extremal elements $\{a, b\}$. S. M. Fallat and J. J. Xing in 2012 proposed the following conjecture: the maximum spread in $S_m[a, b]$ is attained by a rank 2 matrix in $S_m\{a, b\}$. X. Zhan had proved previously that the conjecture was true for $S_m[-a, a]$ with $a > 0$. We will show how to interpret this problem geometrically, via polynomial resultants, in order to be able to treat this conjecture from a computational point of view. This will allow us to prove that this conjecture is true for several formerly open cases.

This is joint work with Neil Calkin, Laureano Gonzalez-Vega, J. Rafael Sendra, and Juana Sendra.

6.2 From Smith forms to spectra to iterative algorithms for sparse integer matrices

Mark Giesbrecht
University of Waterloo, Canada

Integer matrices are often characterized by the lattice of combinations of their rows or columns. This is captured nicely by the Smith canonical form, a diagonal matrix of invariant factors, to which any integer matrix can be transformed through left and right multiplication by unimodular matrices. Algorithms for computing Smith forms have seen dramatic improvements over the past 40 years, but effective algorithms for large sparse matrices still need improvement.

Integer matrices also possess complex eigenvalues and eigenvectors, and every such matrix is similar to a unique one in Jordan canonical form. There is a wealth of numerical methods for computing eigenvalues, and Krylov-type algorithms are effective for sparse matrices.

It would seem a priori that the invariant factors and the eigenvalues would have little to do with each other. Yet we will show that for "almost all" matrices the invariant factors and the eigenvalues are equivalent under a p-adic valuation, in a very precisely counted sense.

A much-hoped-for link is then explored for fast computation of Smith forms of sparse integer matrices, via the better understood algorithms for computing eigenvalues and effective preconditioning.

This is joint work with Mustafa Elsheikh.

6.3 Tools for fast computation of integer matrix normal forms

George Labahn
University of Waterloo, Canada

In this talk we describe a number of tools which are helpful for creating fast algorithms for matrix normal forms of integer matrices. These tools include minimal denominators, Smith massagers,

integer relation bases and partial linearization of integer matrices. This talk should be viewed as an introduction o the later talk by A. Storjohann.

We describe a number of tools used either explicitly or implicitly in a series of papers [1] to [3] for fast computation of Hermite and Smith normal forms of integer matrices. The primary tool used is a Smith Massager, a pair S, F) which for a given nonsingular A allows us to approximate A^{-1} by a rational expression $F \cdot S^{-1}$ with S diagonal.

References

[1] S. Birmpilis, G. Labahn, and A. Storjohann. A Las Vegas algorithm for computing the Smith form of a nonsingular integer matrix. In *Proc. Int'l. Symp. on Symbolic and Algebraic Computation: ISSAC'20*, page 38–45, New York, NY, USA, 2020. ACM.

[2] S. Birmpilis, G. Labahn, and A. Storjohann. A fast algorithm for computing the Smith normal form with multipliers for a nonsingular integer matrix. *Journal of Symbolic Computation*, 116: 146–182, 2023.

[3] Birmpilis, S. and Labahn, G. and Storjohann, A., A cubic algorithm for computing the Hermite normal form of a nonsingular integer matrix, *ACM Transactions of Algorithms*, 19: 1–36, 2023.

6.4 Computing Hermite normal forms of integer matrices faster

Arne Storjohann
University of Waterloo, Canada

The Hermite normal form of a non-singular integer matrix is a triangular form obtained using unimodular row operations. A natural goal from a complexity point of view is to show how to compute the form in about the same number of bit operations as required to multiply together two integer matrices of the same dimension and size of entries as the input matrix. In this talk, I will discuss some of our recent work towards achieving this goal. Some subroutines that we need are fast multiplication of integer matrices with columns having skewed bit-length, and computing the Hermite form of a matrix column-modulo a given Smith form.

6.5 Homotopy Methods for Computing Roots of Mandelbrot Polynomials

Eunice Y. S. Chan
Chinese University of Hong Kong, Shenzhen, China

The Mandelbrot polynomials are recursively defined as:

$$p_0(z) = 1, \quad p_{n+1}(z) = z p_n(z)^2 + 1,$$

and serve as a test problem for exploring the computation of roots in highly structured, recursively defined polynomials. The roots of these polynomials can be computed by constructing a companion matrix, referred to as the Mandelbrot matrix, whose eigenvalues correspond to the roots of the polynomial. The Mandelbrot matrices are recursively defined as:

$$\mathbf{M_{n+1}} = \begin{bmatrix} \mathbf{M_n} & \mathbf{0} & -\mathbf{c}_n \mathbf{r}_n \\ \mathbf{r}_n & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{c}_n & \mathbf{M_n} \end{bmatrix},$$

where $\mathbf{M_1} = [-1]$. The size of $\mathbf{M_n}$ is $d = 2^{n-1}$, and $\mathbf{c}_n$ and $\mathbf{r}_n$ are vectors of size d, given by:

$$\mathbf{c}_n = \begin{bmatrix} -1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \quad \mathbf{r}_n = \begin{bmatrix} 0 & 0 & \cdots & -1 \end{bmatrix}.$$

This talk investigates the use of homotopy methods as a viable approach to compute the eigenvalues of Mandelbrot matrices by exploiting their recursive structure. Homotopy techniques offer a divide-and-conquer framework that deforms a simpler base matrix into the target matrix, enabling symbolic or numerical tracking of eigenvalues across iterations. Additionally, we extend this approach to Mandelbrot-like matrices, such as Fibonacci-Mandelbrot, Narayana-Mandelbrot, and Euclid matrices, which share similar recursive properties. The results highlight the potential of homotopy methods to efficiently solve eigenvalue problems in structured and recursively defined matrices.

6.6 Sparse Interpolation in Chebyshev Basis: Early Termination and Georg Heinig's Toeplitz Solver

Erich Kaltofen
North Carolina State University, USA
Duke University, USA

Ideas by Kaltofen and Yang [ISSAC 2024] for error-correcting interpolation of polynomials that are a sparse linear combination of Chebyshev polynomials have led to a new early termination algorithm for computing the sparsity.

Kaltofen and Lee [JSC 2003] in their early termination algorithms used thresholds to skip over sporadic probabilistic errors. For early termination in sparse Chebyshev interpolation, thresholds need an algorithm to step from a sequence of singular leading principal submatrices of a Toeplitz matrix to the next non-singular leading principal submatrix. For Prony sparse interpolation, the problem is solved by the 1969 Berlekamp-Massey algorithm, and for Chebyshev sparse interpolation by Georg Heinig's 1983 Toeplitz algorithm.

In my talk, I will describe our new early termination algorithm and Heinig's Toeplitz solver from a Berlekamp-Massey algorithmic viewpoint. Heinig's algorithm, which generalizes the classical Toeplitz solvers by Levinson and Durbin, takes quadratic time and requires linear space.

This is joint work with Zhi-Hong Yang at Central South University, China.

SPECIAL SESSION 7

History of Computer Algebra

The ACA conference is now 30 years old. The discipline of computer algebra (and symbolic computation) is considerably older: its roots are really lost to history, if we include the Antikythera Mechanism. That amazing instrument, surely the oldest analogue computer known, was found in 1901 not so very far from the location of this conference. This broad session is not so ambitious as to want to trace all the prehistory of computer algebra, but we do want to capture as much of that history as resides in living memory and in publications since the advent of digital computers. This session could include discussion of the history of the following topics:

- The development of programming languages for computer algebra, e.g. CAMAL and FORMAC
- Applications of computer algebra and symbolic computation, e.g. celestial mechanics and perturbation methods
- Algebraic algorithms such as the Buchberger algorithm
- Foundational algorithms (e.g. Berlekamp's algorithm, or modular methods)
- We informally refer to these topics as being of the heritage of Turing, of Laplace, of Hilbert, and of Tarski.

We define computer algebra and symbolic computation quite broadly and more by exam- ple than by precept: we take, for instance, anything that is the subject of an ISSAC paper or a SIGSAM Bulletin/Communications on Computer Algebra paper or a Journal of Symbolic Computation paper to be "fair game." This is already extremely broad. Finally, although numerals are also symbols, we exclude the history of numerical methods from discussion except insofar as it pertains to exact computation.

There is a recent thorough history of numerical linear algebra by Brezinski, Meurant, and Redivo-Zaglia available from SIAM Books. We hope by this session to spark discussion that leads to a similar volume but for computer algebra and symbolic computation. We hope that each of the speakers at the session at ACA goes on to write a chapter of that future book.

Session organizers

- Robert M. Corless (University of Western Ontario, London, Ontario, Canada)

- William J. Turkel (University of Western Ontario, London, Ontario, Canada)
- Arthur Norman (Cambridge University, UK)

7.1 A personal history with computer algebra

Jürgen Gerhard
Maplesoft, Canada

In this presentation, I will report on my personal journey in the fascinating world of computer algebra, from undergraduate studies until today. Milestones along the way include the first exposure to algebraic extension fields, polynomial factorization, MuPAD, Modern Computer Algebra [1], Maple, Gröbner bases, ordinals, and multivariate limits.

References

[1] Joachim von zur Gathen and Jürgen Gerhard. *Modern Computer Algebra*. Cambridge University Press, 3rd edition, 2013. https://doi.org/10.1017/CBO9781139856065.

7.2 A history of efficiency problems in Maple

Michael Monagan
Simon Fraser University, Canada

The Maple project began in 1980 at the University of Waterloo. The most important design goal was that Maple be powerful, that is, Maple was efficient so that it could handle large inputs and Maple could solve a wide range of algebraic problems.

The early releases of Maple were not particularly efficient. This was not due to poor algebraic algorithms; rather, it had to do with the choice of the data representation for formulas, poor implementations of some systems algorithms, and design choices that resulted in a loss of efficiency. This talk presents seven efficiency problems that arose over Maple's history and some lessons we learned about writing efficient code in practice.

To assess whether today's Computer Algebra Systems are faster than those from the 1980s, we present a timing benchmark comparing the speed of Maxima with Maple, Magma and Singular on factoring determinants of matrices of polynomials.

7.3 Soft Warehouse, Derive and Computer Algebra

David J. Jeffrey
University of Western Ontario, Canada

The Soft Warehouse (SWH) was a leader in developing computer algebra systems that ran on small-memory environments. Long before laptops became affordable, students and teachers could access symbolic computation on the first personal computers. This talk discusses their best-known product `Derive`, while relating some of the history of SWH. Later projects, such as *AskConstants* and *Rubi*, which will also be touched on.

7.4 Symbolic-Numeric Computation

Lihong Zhi
Chinese Academy of Sciences, China

Symbolic-Numeric Computation (SNC) has become a central area within computer algebra, aiming to bridge the gap between exact symbolic methods and efficient numerical techniques. Its historical development reflects a broader trend in the evolution of computer algebra: the pursuit of algorithms that combine mathematical rigor with computational robustness.

The foundations of SNC were laid in the 1960s and 1970s, with the advent of early symbolic computation systems focused on exact algebraic manipulation. As computational demands increased in areas such as robotics, control theory, and computer-aided geometric design, the limitations of purely symbolic or purely numeric approaches became increasingly evident. The 1980s and 1990s marked a turning point, with foundational advances in approximate polynomial GCDs, symbolic-numeric factorization, and hybrid solvers for systems of equations.

In parallel, recent years have witnessed growing interest in the formalization of mathematics, driven by proof assistants such as Lean 4, which enable the precise encoding of mathematical definitions, theorems, and algorithms. While formal verification has traditionally been rooted in pure mathematics, its interaction with symbolic-numeric computation opens a promising new direction. By formalizing key concepts from computational algebraic geometry and numerical analysis, researchers can now verify both the correctness and the stability of hybrid algorithms, a critical step as such methods become increasingly sophisticated and indispensable in applications across optimization, scientific computing, and data science.

This talk will trace the historical development of symbolic-numeric computation, highlight our contributions to the field, and examine how formal systems like Lean 4 may help shape the future of computer algebra.

7.5 30 Years of Applications of Computer Algebra (ACA), A Personal Perspective

Michael J. Wester and Stanly L. Steinberg
University of New Mexico, USA

This is now the 30th meeting of the Applications of Computer Algebra (ACA) conference series. The first took place in Albuquerque, New Mexico, USA, May 16–19, 1995. The chairs were Stanly L. Steinberg and Michael J. Wester. At the time, computer algebra was still fairly young, and the main established CA conference series was ISSAC, which was fairly theoretical. Stan thought it would be good to have an "applications" conference in which developers and users were encouraged to co-mingle, and enlisted me at co-chair. We started out with a few thousand dollar loan from IMACS (International Association for Mathematics and Computers in Simulation), and a couple of US$10K grant proposals. Both proposals were funded, and we had a very successful conference at the University of New Mexico with 93 people in attendance.

Here, we provide a short history of the ACA conference series, with a collection of lessons learned, sprinkled with anecdotes that prompted them.

7.6 60+ years of Applications: a perspective from Reduce

Arthur Norman
Trinity College, Cambridge, UK

This meeting of ACA notes that it represents 30 years of consideration of the Applications of Computer Algebra. Over that time most of the papers will have concentrated on a presentation how some rather specific application has been addressed using computational tools, and while often the progress described will involve devising new or enhancing existing algorithms, the impact of this on Computer Algebra as a whole will not have been considered. This paper reviews the development and growth on one particular algebra system as prompted by the applications made of it. Very often a software base needs time to stabilize (and the underlying computers have needed to become more powerful) before application can become routine. So here I consider the case of Reduce which as a system has a history spanning 60 years – i.e. twice the lifetime of ACA – and I consider how its development over that extended time period has been driven by a wide range of applications, with that activity continuing up to today.

The lessons that I believe can be drawn from this longitudinal study are:

1. In the early years algebra systems provided fairly basic capabilities, but they found that a very broad range of applications were still within their scope because the calculations involved where huge in scale rather than especially technically challenging per se. This is still often the situation today;

2. Successions of users with the particular scientific problems they were working on have set the agenda for system builders and algorithm designers by identifying particular aspects of symbolic computation that those early systems either did not support at all or where performance was a particular concern;

3. Situations where those who had problems to solve have codified and packaged their work and it has been possible to merge that expertise back into the central system have been important over and over again. Anybody who today sorts out an improved way to make progress in some application domain should be encouraged to contribute what they have done for the benefit of others who follow on;

4. Successful transfer from users as above can benefit from an open system where individuals can observe, access and where necessary modify everything, where the challenge of learning how to extend the system is not too severe, where license terms do not intrude and where system portability means that code developed in one arena will readily migrate to all others;

5. The communication channels from users to developers and maintainers may be almost as important as many fine details of a system when it comes to getting support for a project. This can mean that migration between the three communities should be encouraged;

6. The particular system – REDUCE – discussed here at over 60 years old and still under active development as well as use is among the oldest software systems with such a long history. There are significant parts of the core where the almost original code is still in use. Such a long life is surely a symptom of it having got some things right, and so everybody concerned about how long their own legacy of calculated results and contributed code will last might reasonably want to consider how the close interaction between users with challenging applications and those concerned with the central structure of the system has developed;

7. Anybody who builds their work on the basis of computer algebra might consider whether spending money on a commercial system will guarantee the longer term survival and support of that system. At the same time they can consider the investment of time (sometimes their

> own, sometimes graduate students or other juniors) in discovering how to build and maintain an open source system. It may sometimes not be clear which will be the better long term policy.

Perhaps the major point that I hope this paper will bring to readers' attention is that Computer Algebra systems do not need to be thought of as either magic or as black boxes, and that over the years a great deal of their development has been driven by those with an applications focus, so ACA can continue to set priorities for the next enhancements to be made, and it potentially provides a pool of expertise that could be developed to gradually take over system support and to provide guidance to future generations.

7.7 Analysis versus Algebra in Symbolic Computation

Robert M. Corless
University of Western Ontario, Canada

The search for formulaic answers via algebra has an ancient history. That such formulæ may have lacunæ where they do not apply was perhaps first noted explicitly by Cauchy in his 1821 *Cours d'Analyse* (English translation presented at the MacTutor site):

> We must even note that they suggest that algebraic formulas have an unlimited generality, whereas in fact the majority of these formulas are valid only under certain conditions and for certain values of the quantities they contain. By determining these conditions and these values, and by fixing precisely the sense of all the notations I use, I make all uncertainty disappear.

But battle was joined anew when digital computers arrived on the scene. The early generations of software performed pretty well all transformations taking an "algebraic" approach and not considering "analytic" issues[1]. This had consequences: the tension between algebra and analysis continues to this day and many current algebra systems will still sometimes give incomplete, misleading, or flatly incorrect answers to various questions. In this talk I will describe some of the history of how this battle has unfolded in the symbolic computation community. Some good progress has been made, and some of today's algorithms and implementations are genuinely better than most of those of thirty years ago.

7.8 Portability of Early Computer Algebra Systems: First Thoughts

Arthur C. Norman[1] and Stephen M. Watt[2]
[1] Trinity College, Cambridge, UK
[2] University of Waterloo, Canada

We have been involved in the creation of multiple software systems for computer algebra, including Reduce, Maple, Axiom and Aldor as well as a number of smaller specialized programs. We relate some personal observations on how software portability was achieved over from the 1970s to the present day. We focus on the roles of Lisp and the BCPL family of programming languages and provide a demonstration of Reduce as it was in 1973.

[1] I'm not being precise, here. Roughly what I intend to convey by "algebra" versus "analysis" is that algebraic models of computation typically have a different notion of continuity than do analytic models of computation, if they consider continuity at all.

7.9 Symbolic Computation in 1974–1976 in Japan

Tateaki Sasaki
University of Tsukuba, Japan

First, this article surveys the beginning of symbolic computation in Japan which had been led by Prof. Eiich Goto with his paper "Monocopy and Associative Algorithms in an Extended Lisp" named HLISP (for Hash-LISP) written in 1974 (*we can get it from Web*) and the first application of the HLISP to the computation of so-called "Feynman graphs in the QED (= Quantum Electro-Dynamics)" by the speaker in 1975. Reading the Goto's paper, the readers will understand that the HLISP saves the memory as much as possible by avoiding the appearance of duplicated lists by hashing, and they will also think that Prof. Goto was stingy. However, if the readers know that the computer we had used at that time for "large computations" was very restricted in the memory (about 1 Mega-words memory), they will understand why Goto deviced to save the memory severly. In addition, we survey very brie y how the computer algebra had been popularized in 1980's in Japan.

Secondly, this article introduces that Prof. Goto is an unbelievably excellent and fantastic **inventor** (he often called himself not a researcher but an inventor). One influential example is a new electron-beam method to evolve the LSI (Large Scale Integrated-circuit) to the VLSI (V means Very), invented in 1975. The speaker will introduces several of such hardware invented by Goto, as well as a Lisp machine.

SPECIAL SESSION 8

D-Finite Functions and Beyond: Algorithms, Combinatorics, and Arithmetic

D-finite functions are solutions of linear differential equations with rational function coefficients. They form an important class of special functions that appears ubiquitously in algebra, combinatorics, number theory, and beyond. The class is closed under addition and multiplication, derivation and integration, various kinds of coefficient extraction, and under taking diagonals of series. The D-finiteness of generating functions also reflects the complexity of combinatorial classes, with definite relevance in enumeration. This has long made D-finite functions become a standard data structure for the manipulation of special functions in symbolic computation and combinatorics. D-finite functions also admit several extensions amenable to more recent algorithmic treatments, such as DD-finite functions and series defined by quadratic differential equations.

The goal of this special session is to create an exchanging forum for researchers who work on the algorithmic, combinatorial, and arithmetic aspects of D-finite and related functions. It is a continuation of the special sessions that took place in 2022 and 2023.

Session organizers

- Shaoshi Chen (Chinese Academy of Sciences, China)
- Frédéric Chyzak (Inria, France)
- Antonio Jiménez-Pastor (Universidad Politécnica de Madrid, Spain)
- Manuel Kauers (Johannes Kepler University Linz, Austria)
- Veronika Pillwein (Johannes Kepler University Linz, Austria)

8.1 A direct solver for coupled systems of recurrence equations over $\Pi\Sigma^*$-fields

Jakob Obrovsky
Johannes Kepler University Linz, Austria

In this talk I am going to present my work in cooperation with Carsten Schneider on a direct solver for coupled systems of linear higher-order recurrence equations whose coefficients are given in terms of nested sums and products.

One strategy for solving such systems is to first decouple the system [3] and [10] to obtain several scalar equations in only one of the unknowns. These scalar equations then can be solved using the algorithm in [2]. However, this strategy is rather inefficient if the dimension of the system is large [6]. For some cases, algorithms have been developed to avoid decoupling and solve the system in a direct way. These algorithms efficiently find hypergeometric and rational solutions for the rational difference field $K(x)$ with $\sigma(x) = x + 1$ and rational solutions of systems of q-recurrence equations [1], [5] and [8]. We generalized these methods to obtain an algorithm that operates over $\Pi\Sigma^*$-fields [7], incorporating ideas from [4] and [9]. That is, we can directly compute hypergeometric and rational solutions of coupled systems of recurrence equations over $\Pi\Sigma^*$-fields. Within $\Pi\Sigma^*$-fields it is possible to represent indefinitely nested sums and products, thus covering in particular a big class of D-finite sequences.

During the talk I will give a rough overview of the main components of the solver and present examples from the wide range of inputs for which the solver is applicable.

This research was funded in whole or in part by the Austrian Science Fund (FWF) 10.55776/I6130.

Keywords: Coupled Systems, Difference Fields, Rational Solutions, Hypergeometric Solutions

References

[1] Sergei A. Abramov, Moulay A. Barkatou. Rational solutions of first order linear difference systems. *Proceedings of the 1998 International Symposium on Symbolic and Algebraic Computation (ISSAC' 98)*, 124–131, Dublin, 1998.

[2] Sergei A. Abramov, Manuel Bronstein, Marko Petkovšek and Carsten Schneider. On rational and hypergeometric solutions of linear ordinary difference equations in $\Pi\Sigma^*$-field extensions. *Journal of Symbolic Computation*, 107:23–66, 2021.

[3] Moulay A. Barkatou. An algorithm for computing a companion block diagonal form for a system of linear differential equations. *Applicable algebra in engineering, communication and computing*, 4:185–195, 1993.

[4] Moulay A. Barkatou, Thomas Cluzeau, Ali E. Hajj. Simple forms and rational solutions of pseudo-linear systems. *Proceedings of the 2019 International Symposium on Symbolic and Algebraic Computation (ISSAC' 19)*, 26–33, 2019.

[5] Moulay A. Barkatou, Mark van Hoeij, Johannes Middeke, Yi Zhou. Hypergeometric solutions of linear difference systems. *Journal of Symbolic Computation* (2025, to appear).

[6] Alin Bostan, Frédéric Chyzak, Élie De Panafieu. Complexity estimates for two uncoupling algorithms. *Proceedings of the 2013 International Symposium on Symbolic and Algebraic Computation (ISSAC' 13)*, 85–92, Boston, 2013.

[7] Michael Karr. Summation in finite terms. *Journal of the ACM*(JACM), 28(2), 305–350, 1981.

[8] Johannes Middeke. Denominator Bounds and Polynomial Solutions for Systems of q-Recurrences over $K(t)$ for Constant K. *Proceedings of the 2017 International Symposium on Symbolic and Algebraic Computation (ISSAC' 17)*, 325–332, Kaiserslautern, 2017.

[9] Johannes Middeke, Carsten Schneider. Denominator bounds for systems of recurrence equations using $\Pi\Sigma$-extensions. *Waterloo Workshop on Computer Algebra*, 149–173, 2016.

[10] Bruno Zürcher. Rationale Normalformen von pseudo-linearen Abbildungen. *Diplomarbeit Mathematik, ETH Zürich*, 1994.

8.2 Computing D-Finite Symmetric Scalar Products in Order to Count Regular Graphs

Frédéric Chyzak
Inria, France

In this talk I will retrace the evolution of a family of algorithms for computing scalar products between series of the theory of D-finite symmetric functions. I will also describe their application to the computation of differential equations for the generating functions of various classes of regular graphs and generalizations. This culminates with a recent proof of a conjecture on the enumeration of vertex-labeled graphs with allowed degrees 3 and 1 and one more vertex than edges. This is based on joint past and ongoing works with Hadrien Brochet, Hui Hwang, Manuel Kauers, Pierre Lairez, Marni Mishna, and Bruno Salvy.

8.3 Guessing and arithmetic of D-algebraic sequences

Bertrand Teguia Tabuguia[1]
University of Oxford, UK

A sequence is difference-algebraic (or D-algebraic) if finitely many shifts of its general term satisfy a polynomial relationship. We refer to their equations as algebraic difference equations (ADEs). A key motivation for considering nonlinear polynomial equations for sequences is to enable broader closure properties for their symbolic computations. It is well-known that reciprocals and ratios of D-finite sequences are "almost never" D-finite, see Chapter 4 of [5], [2]. We recently proved that any D-finite recurrence can be converted into a non-trivial D-algebraic rational recursion (see (8.1)) using linear algebra [6] and [8].[2]

This talk focuses on arithmetic operations of D-algebraic sequences, building upon ideas presented in [1] and [7]. We aim to present a theoretical framework outlining the necessary hypotheses for constructing ADEs satisfied by sums, products, divisions, and various other operations with D-algebraic sequences. This framework primarily serves to establish the theoretical foundations for these operations, as it relies on computationally intensive elimination with Gröbner bases and is therefore not intended for practical use with generic sequences.

Consider, for instance, the sequence of general term $s_n = \frac{F_n}{C_n}$, where $(F_n)_{n\in\mathbb{N}}$ is the Fibonacci sequence $(F_0 = 0, F_1 = 1, F_{n+2} = F_{n+1} + F_n,\ n \geq 0)$, and $(C_n)_{n\in\mathbb{N}}$ is the Catalan sequence $(C_0 = 1, (n+2)\,C_{n+1} = (4n+2)\,C_n,\ n \geq 0)$. Using the algorithm from [8], we get the following D-algebraic representation for $(C_n)_{n\in\mathbb{N}}$.

$$C_{n+2} = \frac{2C_{n+1}\,(8C_n + C_{n+1})}{10C_n - C_{n+1}},\ C_0 = 1,\ C_1 = 1. \tag{8.1}$$

With this equation, we could employ the Gröbner bases framework to compute an equation satisfied by s_n. Unfortunately for this particular example, these computations did not complete even after an hour on our working computer.

An alternative approach is the guess-and-proof paradigm, which aims to construct the desired equations from the initial terms of $(s_n)_{n\in\mathbb{N}}$. In this case, the correctness is readily verifiable using

[1]The author is supported by UKRI Frontier Research Grant EP/X033813/1.
[2]The next version of [6] is being updated with the complete proof.

the closed forms of F_n and C_n. This method yields a successful result within a second, despite our somewhat 'straightforward' implementation. We obtain a third-order ADE of (total) degree 4.

$$\begin{aligned}
&2240s_{n+2}^3s_{n+1} - 140s_{n+2}^3s_n + 1176s_{n+2}^2s_{n+1}^2 + 52s_{n+2}^2s_{n+1}s_n - 6912s_{n+3}s_{n+2}^2s_{n+1}\\
&+ 2s_{n+2}^2s_n^2 + 544s_{n+3}s_{n+2}^2s_n - 140s_{n+2}s_{n+1}^3 - 27s_{n+2}s_{n+1}^2s_n - 832s_{n+3}s_{n+2}s_{n+1}^2\\
&- s_{n+2}s_{n+1}s_n^2 - 332s_{n+3}s_{n+2}s_{n+1}s_n + 4096s_{n+3}^2s_{n+2}s_{n+1} + 2s_{n+3}s_{n+2}s_n^2 - 512s_{n+3}^2s_{n+2}s_n\\
&- 140s_{n+3}s_{n+1}^3 - 34s_{n+3}s_{n+1}^2s_n + 512s_{n+3}^2s_{n+1}^2 - 2s_{n+3}s_{n+1}s_n^2 - 32s_{n+3}^2s_{n+1}s_n - 4s_{n+3}^2s_n^2 = 0.
\end{aligned} \tag{8.2}$$

We will detail the underlying method. This is our first step toward finding more effective algorithms for the arithmetic of D-algebraic sequences. Similar approaches can be found in [3]. Future developments could exploit the more advanced guessing techniques described in [4].

Keywords: Algebraic difference equation, D-algebraic guessing, elimination with Gröbner bases

Acknowledgment. The author is supported by UKRI Frontier Research Grant EP/X033813/1.

References

[1] Ait El Manssour, R., Sattelberger, A.L., Teguia Tabuguia, B.: D-algebraic functions. Journal of Symbolic Computation p. 102377 (2024)
[2] Gerhold, S.: Combinatorial Sequences: Non-Holonomicity and Inequalities. Phd thesis, Johannes-Kepler-Universität Linz (2005), available at `https://fam.tuwien.ac.at/~sgerhold/pub_files/diss.pdf`
[3] Hebisch, W., Rubey, M.: Extended rate, more GFUN. Journal of Symbolic Computation **46**(8), 889–903 (2011)
[4] Kauers, M., Koutschan, C.: Guessing with little data. In: Proceedings of the 2022 International Symposium on Symbolic and Algebraic Computation. pp. 83–90 (2022)
[5] Van der Put, M., Singer, M.F.: Galois Theory of Difference Equations. Springer (2006)
[6] Teguia Tabuguia, B.: Computing with D-algebraic sequences. arXiv preprint arXiv:2412.20630 (2024)
[7] Teguia Tabuguia, B.: Arithmetic of D-algebraic functions. Journal of Symbolic Computation **126**, 102348 (2025)
[8] Teguia Tabuguia, B., Worrell, J.: On rational recursion for holonomic sequences. In: International Workshop on Computer Algebra in Scientific Computing. pp. 314–327. Springer (2024)

8.4 Integro-differential rings and generalized shuffle relations

Clemens G. Raab[1] and Georg Regensburger[2]
[1] RICAM, Austrian Academy of Sciences, Austria
[2] University of Kassel, Germany

In this talk, we discuss the fundamental theorem of calculus and its algebraic implications in differential rings, allowing for functions with singularities and a generalized notion of evaluation. We give an overview of integro-differential rings and present several examples. This approach generalizes results such as shuffle relations for nested integrals and the Taylor formula, incorporating additional terms to account for singularities [1].

In general, not every element of a differential ring has an antiderivative in the same ring. Starting from a commutative differential ring and a direct decomposition into integrable and non-integrable elements, we outline aspects of the construction of the free integro-differential ring [2]. This integro-differential closure contains, in particular, all nested integrals over elements of the original differential ring.

References

[1] C.G. Raab and G. Regensburger. The fundamental theorem of calculus in differential rings. *Adv. Math.*, 447:109676, 2024.

[2] C.G. Raab and G. Regensburger. The integro-differential closure of a commutative differential ring. In preparation, 2025.

8.5 A MacMahon Partition Analysis View of Cylindric Partitions

Ali K. Uncu
University of Bath, UK

In this talk, we first give a brief introduction about the Rogers-Ramanujan identites and some generalizations of the same type, we also define cylindric partitions and explain their connections with the Rogers-Ramaujan type identities. We will then focus on solving q-recurrences and discovery formulas for a D-finite family of functions which are finite forms of the generating functions through an application of MacMahon's partition analysis on cylindric partitions.

8.6 Conservative Matrix Fields - Algebra and Asymptotics

Shachar Weinbaum
Technion - Israel Institute of Technology, Israel

D-finite sequences, also known as Holonomic or P-recursive sequences, are a family of special functions, which are ubiquitous in many areas of mathematics. The asymptotic properties of these sequences were detailed in landmark papers by Poincare [1] and Perron [2]. Notably, ratios of D-finite sequences satisfying the same recurrence, also known as Apéry limits, are at the core of many irrationality results [3] to [7]. However, finding such sequences with desirable limits and irrationality measures remains a challenge.

In this talk we introduce an interesting object, the Conservative Matrix Field. This object has been used in identity proofs [8], in Diophantine approximations, [9], and most recently for unifying hundreds of formulas for π [10] (see Figure 8.1). We will discuss how this object generates a high dimensional generalization of Apéry limits, by deriving such a sequence from each rational direction in $\mathbb{R}^d$. This generalization keeps the desirable properties of Apéry limits, yet simplifies the search for useful ones. More concretely, experimental analysis suggests the irrationality measure of the Apéry limits is continuous with respect to direction, while the actual sequence limit remains constant (see Figure 8.2). This surprising phenomenon allows for optimization-based search algorithms, such as gradient descent, to be used in the search for irrationality proving approximations.

We will present how Conservative Matrix Fields can be constructed using ideals of finite codimension in an Ore algebra (such as annihilators of D-finite functions), as well as their interesting phenomenological properties. Finally, we will update about our currently ongoing effort to prove these properties.

References

[1] Henri Poincaré. Sur les équations linéaires aux différentielles ordinaires et aux différences finies. *American Journal of Mathematics*, 1885.

[2] Oskar Perron. Über Summengleichungen und Poincarésche Differenzengleichungen. *Mathematische Annalen*, 1921.

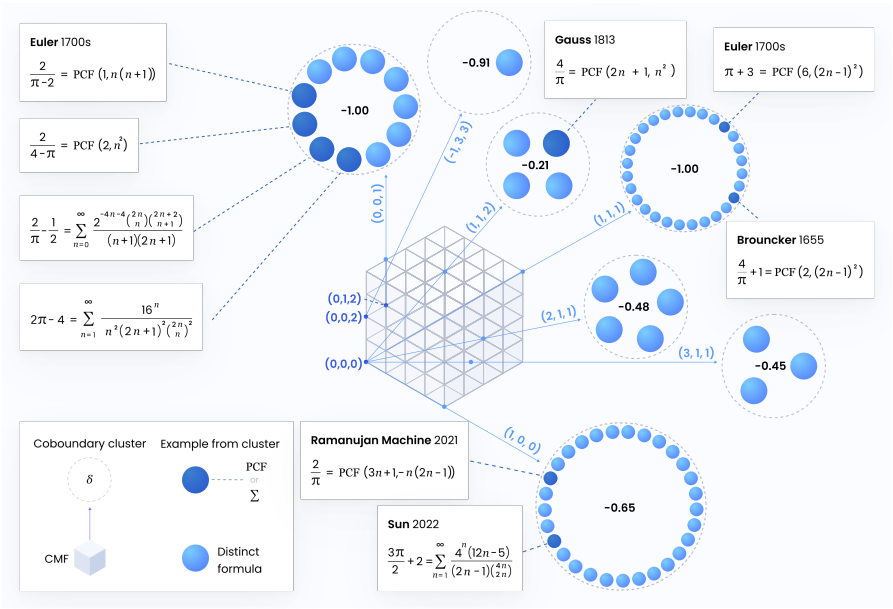


Figure 8.1: **Formula unification by a Conservative Matrix Field**. Numerous π formulas harvested from the literature are automatically arranged as directions in a Conservative Matrix Field defined over $\mathbb{Z}^3$. These formulas include famous ones by Gauss, Euler, and Lord Brouncker. More details available at [10]

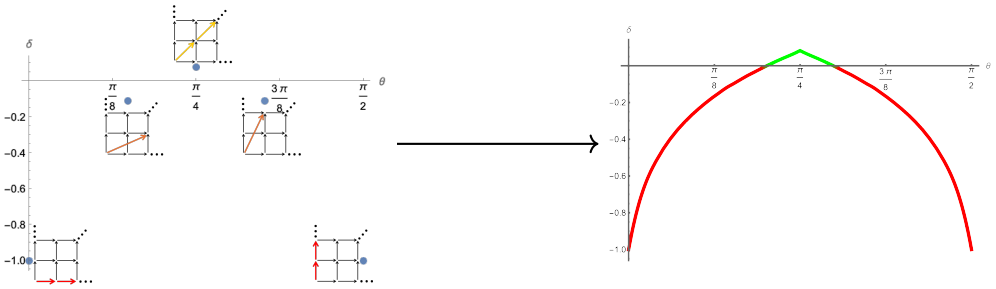


Figure 8.2: **Demonstration of the continuity phenomenon of the irrationality measure**, shown for a Conservative Matrix Field defined on $\mathbb{Z}^2$; the sequences resulting from it converge to $\zeta(3)$. **Left**: a graph of 5 angles, and the estimated irrationality measure of the Diophantine approximations associated with them in the Conservative Matrix Field. Over each data point is a sketch of the angle in $\mathbb{Z}^2$. **Right**: an interpolation of the irrationality measures of a few dozen different angles, demonstrating its surprising continuity. Positive values of δ are in green as they indicate these directions generate sequences that prove irrationality.

[3] Roger Apéry. Irrationalité de $\zeta(2)$ et $\zeta(3)$. *Astérisque*, 1979.

[4] Marc Chamberland and Armin Straub. Apéry Limits: Experiments and Proofs. *The American Mathematical Monthly*, 2021.

[5] Francis Brown and Wadim Zudilin. On cellular rational approximations to $\zeta(5)$. `arXiv:2210.03391`, 2022.

[6] Wadim Zudilin. An Apéry-like difference equation for Catalan's constant. `arXiv:math/0201024`, 2002.

[7] A. I. Aptekarev. On linear forms containing the Euler constant. `arXiv:0902.1768`, 2009.

[8] William Gosper. Strip Mining in the Abandoned Orefields of Nineteenth Century Mathematics *Computers In Mathematics*, 1990.

[9] Rotem Elimelech et al. Algorithm-assisted discovery of an intrinsic order among mathematical constants.

Proceedings of the National Academy of Sciences, 2024.
[10] Tomer Raz et al. From Euler to AI: Unifying Formulas for Mathematical Constants. arXiv:2502.17533, 2025.

8.7 Non-Minimality of Minimal Telescopers Explained by Residues

Manuel Kauers
Johannes Kepler University, Austria

Joint work with Shaoshi Chen, Christoph Koutschan, Xiuyun Li, Ronghua Wang, and Yisen Wang

We will report on our joint ISSAC'25 paper. In this paper, elaborating on an approach recently proposed by Mark van Hoeij, we continue to investigate why creative telescoping occasionally fails to find the minimal-order annihilating operator of a given definite sum or integral. We offer an explanation based on the consideration of residues.

8.8 A purity theorem for Mahler equations

Julien Roques
Université Lyon 1, France

Let $p \geq 2$ be an integer. This talk concerns (linear) p-Mahler equations, *i.e.*, linear functional equations of the form

$$a_0(z)f(z) + a_1(z)f(z^p) + \cdots + a_d(z)f(z^{p^d}) = 0, \tag{8.3}$$

where the coefficients $a_0, \ldots, a_d$ belong to $\overline{\mathbb{Q}}(z)$ and satisfy $a_0 a_d \neq 0$. For instance, the generating series of p-automatic sequences—or more generally, of p-regular sequences—satisfy such equations.

Hahn series play a key role in the study of p-Mahler equations. Roughly speaking, Hahn series generalize Puiseux series by allowing arbitrary rational exponents of the indeterminate, provided that the set that supports them is well-ordered. Their significance in our context is made clear by the following result: the difference field $(\mathscr{H}, \varphi_p)$, where $\mathscr{H} = \overline{\mathbb{Q}}((z^{\mathbb{Q}}))$ is the field of Hahn series with coefficients in $\overline{\mathbb{Q}}$ and value group $\mathbb{Q}$ and where φ_p is the field automorphism of $\mathscr{H}$ sending $f(z)$ on $f(z^p)$, has a difference ring extension $(\mathcal{R}, \varphi_p)$ with field of constants $\mathcal{R}^{\varphi_p} = \{f \in \mathcal{R} \mid \varphi_p(f) = f\}$ equal to $\overline{\mathbb{Q}}$ such that

- for any $c \in \overline{\mathbb{Q}}^\times$, there exists $e_c \in \mathcal{R}^\times$ satisfying $\varphi_p(e_c) = ce_c$;
- there exists $\ell \in \mathcal{R}$ satisfying $\varphi_p(\ell) = \ell + 1$;
- any p-Mahler equation of the form (8.3) has d solutions $y_1, \ldots, y_d \in \mathcal{R}$ that are $\overline{\mathbb{Q}}$-linearly independent and of the form

$$y_i = \sum_{(c,j) \in \overline{\mathbb{Q}}^\times \times \mathbb{Z}_{\geq 0}} f_{i,c,j} e_c \ell^j, \tag{8.4}$$

  where the sum has finite support and the $f_{i,c,j} \in \mathscr{H}$ satisfy p-Mahler equations.

In this talk, we will focus on the growth of the logarithmic Weil height of the coefficients of the Hahn series that arise when solving p-Mahler equations. We will report on recent joint work with C. Faverjon, in which:

- we show that five distinct asymptotic growth behaviors can occur, thereby generalizing a previous result by B. Adamczewski, J. P. Bell, and D. Smertnig about p-Mahler series;
- we establish a purity theorem reminiscent of classical purity theorems for G-functions due to D. and G. Chudnovsky, and for E-functions (and more generally, for holonomic arithmetic Gevrey series) due to Y. André.

8.9 Non-commutative D-finite & D-algebraic power series and formal languages

Robert Green and Joshua Grochow
University of Colorado, USA

We define and study non-commutative analogues of multivarite D-finite and D-algebraic generating functions, and the complexity classes of languages corresponding to them. In particular, we give both equational (fixed point) characterizations and automata machine model characterizations of these classes, and relate them to standard language classes (regular, linear, context-free, and tree-adjoining). We prove several inclusions and separations between our new classes and each other, and our new classes and classical language classes. Among our more surprising results are:

- Left D-finite and right D-finite languages are not the same, unlike the case of left linear and right linear (which both give exactly the regular languages).
- There are non-commutative algebraic power series (corresponding to CFLs) that are not D-finite, in contrast to the classical theorem that commutative algebraic power series are D-finite.
- There are left D-finite languages that are not even tree-adjoining, and there are tree-adjoining languages that are not even D-algebraic.

In addition to proving many results on these classes, we also highlight many open questions ripe for future research.

SPECIAL SESSION 9

Algebraic geometry from an algorithmic point of view

From the end of the 19th century to most of the 20th century several mathematicians made a conscious effort to avoid constructive arguments, emphasizing existential methods instead. The final decades of the 20th century witnessed a return to a constructive approach.

In this context, Computer Algebra grew up as a branch of mathematics and computer science that focuses on the development and implementation of algorithms and software systems to perform symbolic mathematical computations, also with a promotion of interactions with different topics, such as Algebraic Geometry and Commutative Algebra.

The first obvious reason of this interplay is that algorithms allow the construction of examples, from which researchers can deduce possible solutions to the questions they deal with. In this context, the necessity to design new algorithms for specific topics of interest or to optimize the existing ones often arises. Indeed, several existing algorithms theoretically allow some explicit computations (e.g. Groebner Bases), but in practice they do not give the desired result in a reasonable time, or using a reasonable amount of memory. The second less obvious reason is that projecting an algorithm can give a new insight in the problem one is trying to solve.

This synergy creates a virtuous cycle, where the development of Computer Algebra systems drives new mathematical discoveries, which in turn inspire further innovations in algorithm design. This session focuses on investigations in Algebraic Geometry from a computational point of view and on possible consequent applications in other fields (e.g. coding theory, cryptography, computer graphics). Hence, it aims at gathering specialists from different areas (Algebraic Geometry, Commutative Algebra, Computer Algebra, Applied Mathematics) and discuss interactions between them. Expected topics of presentations include (but are not limited to):

- algebraic and combinatorial aspects of problems in Algebraic Geometry;
- algorithms and constructive methods for Algebraic Geometry and applications;
- implementation of algorithms and optimization, possibly with comparisons with existing ones.

Session organizers

- Cristina Bertone (Dipartimento di Matematica G. Peano, Università di Torino, Italy)

- Francesca Cioffi (Dipartimento di Matematica e Applicazioni R. Caccioppoli, Università di Napoli Federico II, Italy)

9.1 Computational Classification and Generation of Algebraic Surfaces and Curves via Algorithms

Meirav Amram
Shamoon College of Engneering, Israel

We present algebraic, geometric, topological and algorithmic methods in the classification of algebraic surfaces and curves. We present recent research and softwares; one of them helps in finding Zariski pairs.

9.2 On the shape of Betti diagrams of edge ideals

Sara Asensio
University of Valladolid, Spain

Since edge ideals were first introduced in 1990, they have been a clear example of the connection between commutative algebra and graph theory. In this talk, we will focus on the study of Betti diagrams of this type of ideals using a combination of homological and combinatorial tools that allow us to take advantage of the properties of some associated graphs. In particular, we will provide families of graphs whose associated edge ideals have somehow special characteristics.

9.3 Khovanskii bases in computer algebra

Barbara Betti[1], Viktoriia Borovik[2], Leonie Kayser[1], Marta Panizzut[3] and Simon Telen[1]
[1] Max Planck Institute for Mathematics in the Sciences, Leipzig, Germany.
[2] University of Osnabrück, Germany.
[3] UiT - The Arctic University of Norway, Tromso, Norway

In this talk we will recall the definition of Khovanskii bases, also known as Sagbi bases, and make a parallel with properties of Gröbner bases. Inspired by several applications of Gröbner bases in solving 0-dimensional polynominal systems, we will provide analogous applications in computer algebra using Khovanskii bases. These include the introduction of an eigenvalue algorithm based on the assumption that the equations are homogeneous with respect to a finite Khovanskii basis and homotopy continuation methods that exploit toric degenerations.

9.4 Solving parametric polynomial systems using generic Rational Univariate Representation

Corniquel Florent
IMJ-PRG and INRIA Paris, France

Given $f_1, \ldots, f_n \in \mathbb{Q}[W, X]$ where $W = [W_1, \ldots, W_s]$ is a list of parameters and $X = [X_1, \ldots, X_n]$ a list of indeterminates, we propose an extension of the Rational Univariate Representation (RUR) to parametric systems that are zero-dimensional for almost all values of parameters.

9.5 Homogenous Instanton Bundles on Grassmannians

Özhan Genç
Jagiellonian University, Poland

We will provide a full classification of irreducible homogeneous h-instanton bundles on a Grassmannian $G = \mathrm{Gr}(k, n)$ where h is the hyperplane section of G equipped with the Plücker embedding.

9.6 Computational Generation of Zariski Pairs in Conic-Line Arrangements

Gal Goren
Technion Institute of Technology, Israel

In this talk, we focus on Zariski pairs arising in arrangements of a conic and n lines, presenting a computational approach to identifying all such pairs for given values of n.

9.7 Gröbner bases native to finitely generated commutative algebras with term order, with application to the Hodge algebra of minors

Abhiram Natarajan
University of Warwick, UK

Standard Gröbner basis methods are often too inefficient to handle even small cases arising in areas such as computational complexity theory—for instance, the orbit closure of the 3×3 determinant in geometric complexity theory. Motivated by this, we develop a theory of Gröbner bases tailored to algebras with straightening law (ASLs, or Hodge algebras), and more generally to any finitely generated commutative algebra over a field $\mathbb{F}$ admitting a suitable term order. We instantiate this theory in the bideterminant ASL on a polynomial ring—generated by products of minors of a variable matrix—defining what we call bd-Gröbner bases. This framework packages several results on bideterminants in a clean form, including a one-line proof of a bd-Gröbner basis for the ideal of t-minors for any t, which is universal in our sense. While ordinary Gröbner bases for such ideals are known, their proofs are more involved.

9.8 The Gröbner basis for powers of a general linear form in a monomial complete intersection

Filip Jonsson Kling*, Samuel Lundqvist*, Fatemeh Mohammadi** and Matthias Orth**,[1]
* Stockholm University, Sweden
** KU Leuven, Belgium

[1]M. Orth (presenter of talk) was partially supported by the FWO grants G0F5921N (Odysseus) and G023721N, and by the KU Leuven grant iBOF/23/064.

In a polynomial ring over a field of characteristic zero, we study almost complete intersection ideals generated by powers of the variables and a power of the sum of the variables. Using a lower bound for the Hilbert series of the quotient rings defined by almost complete intersections, we obtain all reduced Gröbner of any such almost complete intersection ideal. Our method is mainly combinatorial in nature, as we focus on an analysis of the initial ideal. With any monomial in the vector space basis of an Artinian monomial complete intersection, we associate a lattice path, and introduce a reflection operation on these paths that allows for a crucial counting argument. In particular we obtain a new proof for the fact that Artinian monomial complete intersections have the strong Lefschetz property over fields of characteristic zero.

9.9 The moduli space of rational elliptic surfaces

Simone Pesatori
University of Roma Tre, Italia

We generalize the notion of resultant of two polynomials and stratify the space of pairs of homogeneous polynomials in two complex variables in terms of the multiple and common roots they have. As an application, we stratify the boundary of the moduli space of rational elliptic surfaces in terms of the configurations of singular fibers the surfaces admit. We explain the limitation of our machinery and how a computational method could solve it.

9.10 A computer-aided construction of non-homeomorphic double Kodaira fibrations that possess the same biregular invariants

Pietro Sabatino
Institute for High Performance Computing and Networking (ICAR-CNR), Italy

Let Σ_b be a closed Riemann surface of genus b. We investigate finite quotients G of the pure braid group on two strands $\mathsf{P}_2(\Sigma_b)$ that do not factor through $\pi_1(\Sigma_b \times \Sigma_b)$. Building on previous work on special systems of generators on finite groups called *diagonal double Kodaira structures*, we prove that if G has not order 32, then $|G| \geq 64$. We completely classify the cases where equality holds (see [8]). As a geometric application of these algebraic results, we construct two 3-dimensional families of double Kodaira fibrations with the same biregular invariants and Betti numbers but different fundamental groups. When investigating groups of order 64, the computational algebra system `GAP4` is central to our approach. Code is available on GitHub, [5]. This is a joint work with Francesco Polizzi.

Acknowledgements

The author was supported by project FAIR (Future AI Research), under program NRRP MUR funded by EU-NGEU (PE00000013)

References

[1] W. Barth, K. Hulek, C.A.M. Peters, A. Van de Ven, *Compact Complex Surfaces.* Grundlehren der Mathematischen Wissenschaften, Vol **4**, Second enlarged edition, Springer-Verlag, Berlin, 2003.

[2] F. Catanese: Kodaira fibrations and beyond: methods for moduli theory, *Japan. J. Math.* **12** (2017), no. 2, 91–174.
[3] A. Causin, F. Polizzi: Surface braid groups, finite Heisenberg covers and double Kodaira fibrations, *Ann. Sc. Norm. Super. Pisa Cl. Sci.* Vol. **XXII** (2021), 1309-1352
[4] The GAP Group, *GAP – Groups,Algorithms, and Programming, Version 4.11.1*; 2021.
[5] `https://github.com/pietros16bit/gap4ddks`
[6] D. L. Gonçalves, J. Guaschi: On the structure of surface pure braid groups, *J. Pure Appl. Algebra* **186** (2004), 187–218.
[7] F.Polizzi, P. Sabatino: Extra-special quotients of surface braid groups and double Kodaira fibrations with small signature, *Geom. Dedicata* **216**, 65 (2022)
[8] F.Polizzi, P. Sabatino: Groups of order 64 and non-homeomorphic double Kodaira fibrations with the same biregular invariants, *arXiv*: `https://arxiv.org/abs/2412.08260`, (2024)

9.11 Deterministic Determination of Axial Constants and Sectional Regularities

Amir Hashemi[1], Rozhin Sadr[2] and Werner M. Seiler[2]
[1] Isfahan Technical University, Iran
[2] Kassel University, Germany

We consider some generic notions in algebraic geometry, axial constants, sectional regularity and generic annihilator numbers, and related them to deterministic notions of genericity to make them effectively computable. Our approach is based on the theory of Pommaret bases.

9.12 Improving convex-dense bivariate factorization

Martin Weimann
Université Caen Normandie, France

We propose a new algorithm for factoring a bivariate polynomial $F \in \mathbb{K}[x, y]$ which takes fully advantage of the geometry of the Newton polygon of F. Under some non degeneracy hypothesis, the complexity is $\tilde{\mathcal{O}}(Vr_0^{\omega-1})$ where V is the volume of the polygon and r_0 is its minimal lattice length, an easy-to-compute upper bound for the number of indecomposable Minkovski summands. The proof is based on a new fast factorization algorithm in $\mathbb{K}[[x]][y]$ with respect to an augmented valuation, a result which has its own interest.

9.13 Geometric Foundations for Transformer in Gröbner Basis Computation

Yuta Kambe[1], Yota Maeda[2,3] and Tristan Vaccon[4]
[1] Mitsubishi Electric, Japan
[2] Technische Universität Darmstadt, Germany
[3] Tohoku University, Japan
[4] Université de Limoges, France

We provide a theoretical foundation for Transformer-based computation of Gröbner bases by proving the geometric generality of existing dataset generation algorithms and introducing an

extended sampling method. Under a mild heuristic and assuming a Hilbertian base field, we show that the training examples constructed via random elementary matrix transformations are Zariski dense in the space of generating sets of a fixed ideal. This guarantees that Transformers trained on such data can, in principle, learn any generic Gröbner basis. Our extended algorithm controls sparsity, interaction, and coefficient distributions, further improving dataset richness and empirical performance.

9.14 Combinatorics of Schubert Cells in Random Network Coding

Alessandro Neri
University of Naples Federico II, Italy

In 2009 Etzion and Silberstein provided a combinatorial upper bound on the largest dimension of a space of matrices over a finite field whose nonzero matrices are supported on a given Ferrers diagram and all have rank lower bounded by a fixed positive integer r. In the same paper, they also conjectured that such an upper bound is always tight. Since then, their conjecture has been verified in a number of cases, but as of today it still remains widely open. In this work, we investigate the notion of reducibility of Ferrers diagrams: a diagram $\mathcal{D}$ reduces to $\mathcal{D}'$ if an optimal matrix space supported on $\mathcal{D}$ can be obtained by shortening and/or inclusion of an optimal matrix space supported on $\mathcal{D}'$. This induces a natural notion of irreducibility of Ferrers diagrams, and the validity of the conjecture for irreducible diagrams implies the validity of the full conjecture. Moreover, following this notion, we can provide the Hasse diagram of Young's lattice with an orientation. This produces a directed graph in which sources correspond to irreducible diagrams. This is a Joint work with Hugo Sauerbier Couvée.

9.15 Constructing nonspecial divisors in the moduli space of cubic fourfolds

Elena Sammarco
Università degli studi Roma Tre, Italia

We present a geometric approach to construct some nonspecial divisors in the moduli space of cubic fourfolds and the possibility to generalize it using computational methods applied to explicit equations. Furthermore, we raise the question of determining whether, given a cubic fourfold with a specific equation, it belongs to the divisors just defined.

SPECIAL SESSION 10

Algebraic and Algorithmic Aspects of Differential and Integral Operators Session

The algebraic/symbolic treatment of differential equations is a flourishing field, branching out in a variety of subfields committed to different approaches. In this session, we want to give special emphasis to the operator perspective of both the underlying differential operators and various associated integral operators.

In particular, we invite contributions in line with the following topics:

- Symbolic Computation for Operator Algebras
- Factorization of Differential/Integral Operators
- Linear Boundary Problems and Green's Operators
- Initial Value Problems for Differential Equations
- Symbolic Integration and Differential Galois Theory
- Symbolic Operator Calculi
- Algorithmic D-Module Theory
- Rota-Baxter Algebra
- Differential Algebra
- Discrete Analogs of the above
- Software Aspects of the above

Previous ACA sessions were held at

- Hagenberg 2008
- Montréal 2009
- Vlora 2010
- Houston 2011
- Sofia 2012
- Malaga 2013
- New York 2014
- Kalamata 2015
- Kassel 2016
- Santiago de Compostela 2018

- Montréal 2019
- ONLINE 2021,
- Warsaw 2023

We have published an MCS Special Issue based on the 2008-10 sessions and a Springer LNCS Post-proceedings Volume based on the 2011-12 sessions.

We have co-edited a Special Issue with Alexey Ovchinnikov on Computational Aspects of Differential/Difference Algebra and Integral Operators for the journal Advances in Applied Mathematics based on ACA 2014 and 15.

Session organizers

- Moulay Barkatou (University of Limoges, XLIM, France)
- Thomas Cluzeau (University of Limoges, CNRS, XLIM, France)
- Clemens Raab (RICAM, Austrian Academy of Sciences, Linz, Austria)
- Georg Regensburger (University of Kassel, Germany)

10.1 The indicial equation of the product of linear ordinary differential operators

Sergei A. Abramov
Russian Academy of Sciences, Russia

The roots of the indicial equation, constructed for a given linear ordinary differential operator, provide an important information on the solutions of the corresponding homogeneous differential equation. Operators are considered whose coefficients are formal Laurent series. The structure of the indicial equation of the product of given differential operators is described.

10.2 Separated Variables on Plane Algebraic Curves

Manfred Buchacher
Johannes Kepler Universität Linz, Austria

We consider equations of the form

$$r(x, y) + q(x, y)p(x, y) = f(x) - g(y),$$

for rational functions $r(x, y)$, $q(x, y)$, $p(x, y)$, $f(x)$ and $g(y)$ in x and y over $\mathbb{K}$, and explain how they can be solved based on the ideas developed in [1] to [3]. The procedure we present reduces the non-linear problem to a linear one. However, the procedure is just a semi-algorithm. It terminates, whenever the equation has a non-trivial solution, but it may not, if there is none. Termination depends on a dynamical system on the curve associated with p and the location of the poles of r thereon. It is still an open question how the semi-algorithm could be turned into an algorithm.

The problem has a field theoretic interpretation. Let $\mathbb{K}(x, y)$ be the field generated by elements x and y satisfying the (only) relation $p(x, y) = 0$, and let $\mathbb{K}(x)$ and $\mathbb{K}(y)$ be the subfields generated by x and y, respectively. Then the above equation has a (non-trivial) solution if and only if $r(x, y)$ is an element of $\mathbb{K}(x) + \mathbb{K}(y)$. There are two particular cases that are interesting in themselves: the case $r = 0$, and the case $g = 0$. The former corresponds to the problem of computing the intersection of $\mathbb{K}(x)$ and $\mathbb{K}(y)$, the latter to the problem of deciding whether $r(x, y)$ is an element of $\mathbb{K}(x)$ and finding all representations thereof in terms of x.

The problem arises in enumerative combinatorics, when solving discrete differential equations by reducing partial DDEs to systems of ordinary ODDEs [4]. It also arises in parameter-identification problems in ODE models [5], and in problems of image recognition [6].

References

[1] Manfred Buchacher, Manuel Kauers, and Gleb Pogudin. Separating Variables in Bivariate Polynomial Ideals. *Proceedings of the 45th International Symposium on Symbolic and Algebraic Computation*, pages 54-61, 2020.

[2] Manfred Buchacher. Separating Variables in Bivariate Polynomial Ideals: the Local Case. *arXiv preprint*, arXiv:2404.10377, 2024.

[3] Manfred Buchacher. Separated Variables on Plane Algebraic Curves. *arXiv preprint*, arXiv:2411.08584, 2024.

[4] Olivier Bernardi, Mireille Bousquet-Mélou, and Kilian Raschel. Counting quadrant walks via Tutte's invariant methods. *Discrete Mathematics & Theoretical Computer Science*, 2020.

[5] Alexey Ovchinnikov, Anand Pillay, Gleb Pogudin, and Thomas Scanlon. Computing all identifiable functions of parameters for ODE models. *Systems & Control Letters*, 2021.

[6] Anna Katherina Binder. Algorithms for Fields and an Application to a Problem in Computer Vision. *PhD Thesis.* Technische Universität München, 2009.

10.3 Topological closure of formal powers series ideals and application to topological rewriting theory

Cyrille Chenavier
University of Limoges, France

We will present the paper [1], where we investigate formal power series ideals and their relationship to topological rewriting theory. Since commutative formal power series algebras are Zariski rings, their ideals are closed for the adic topology defined by the maximal ideal generated by the indeterminates. In [1], we provide a constructive proof of this result which, given a formal power series in the topological closure of an ideal, consists in computing a cofactor representation of the series with respect to a standard basis of the ideal. We apply this result in the context of topological rewriting theory, where two natural notions of confluence arise: topological confluence and infinitary confluence; in general, infinitary confluence is a strictly stronger notion than topological confluence. Using topological closure of ideals, we finally show that in the context of rewriting theory on commutative formal power series, infinitary and topological confluences are equivalent when the monomial order considered is compatible with the degree.

References

[1] Cyrille Chenavier, Thomas Cluzeau and Adya Musson-Leymarie. Topological closure of formal powers series ideals and application to topological rewriting theory. *J. Symbolic Comput.*, 2025.

10.4 Hypergeometric solutions of elliptic difference equations

Thierry Combot
University of Bourgogne, France

In this presentation, we will present an algorithm to compute hypergeometric solutions of a linear difference equation on an elliptic curve.

Consider an elliptic curve $\mathcal{C}$ with coefficients in $\overline{\mathbb{Q}}$ and $\delta \in \mathcal{C}(\overline{\mathbb{Q}})$ a non torsion point. We consider an elliptic difference equation $\sum_{i=0}^{l} a_i(p) f(p \oplus i.\delta) = 0$ with $\oplus$ the elliptic addition law and a_i polynomials on $\mathcal{C}$. We present an algorithm to compute rational solutions, then an intermediary class we call pseudo-rational solutions, and finally hypergeometric solutions, which are functions f such that $f(p \oplus \delta)/f(p)$ is rational over $\mathcal{C}$.

References

[1] Thierry Combot. Hyperexponential solutions of elliptic difference equations, 29 Apr 2022. `https://arxiv.org/abs/2205.00041`.

10.5 An Effective Version of the Grothendieck p-curvature Conjecture for Order One Differential Equations

Florian Fürnsinn
University of Vienna, Austria

To a linear differential equation with polynomial coefficients over the rational numbers one can attach, for all prime numbers p, a linear map called the *p-curvature*. The Grothendieck p-curvature conjecture asserts that the algebraicity of a full basis of solutions of such a differential equation is equivalent to the vanishing of the p-curvatures for almost all prime numbers p. In 1974 Honda provided a proof of this conjecture for order one equations [2], by reducing the problem to a theorem of Kronecker [3], which provides a local-global criterion for the splitting of polynomials over the rational numbers. In 1985 Chudnovsky and Chudnovsky gave a new proof of Kronecker's result [1], and with it of Honda's result, using Padé approximation.

In this talk I will explain how to use the proof of the Chudnovsky brothers to make Honda's result effective. More precisely, given a linear differential equation of order one with polynomial coefficients over the rational numbers we deduce an upper bound on the number of p-curvatures to be computed in order to decide the algebraicity of all solutions of the equation.

This talk is based on ongoing joint work with Lucas Pannier.

References

[1] David V. Chudnovsky and Gregory V. Chudnovsky. Applications of Padé approximations to the Grothendieck conjecture on linear differential equations. *Number theory* (New York, 1983–84). Vol. 1135. Lecture Notes in Math. Springer, Berlin, 1985, pp. 52–100.

[2] Taira Honda. Algebraic differential equations. *Symposia Mathematic.*, Vol. XXIV (Sympos., INDAM, Rome, 1979). London-New York: Academic Press, 1981, pp. 169–204.

[3] Leopold Kronecker. Über die Irreducibilität von Gleichungen *Monatsberichte der Königlichen Preussische Akademie des Wissenschaften zu Berlin* (1880), pp. 155–163.

10.6 The Shimizu–Morioka System Has No Nontrivial Darboux Polynomials

Khalil Ghorbal
Inria, France

In 1980 Shimizu and Morioka [3] presented a simple three dimensional ordinary differential equation as a model to study the convection of turbulent flows (i.e. flows with high Rayleigh numbers). More recently, Huang et al. [2] studied the Darboux integrability of the system and showed that it has no nontrivial Darboux polynomial of total degree less than four. They further conjectured that the system has no nontrivial Darboux polynomial for any positive total degree. We prove that this is indeed the case leveraging our seminal work on using the concept of *generic polynomials* to systematically study the existence of Darboux polynomials [1].

This is a joint work with Maxime Bridoux (Inria, France).

References

[1] Khalil Ghorbal and Maxime Bridoux. Automated reasoning for the existence of darboux polynomials. In *Proceedings of the 2024 International Symposium on Symbolic and Algebraic Computation*, page 324–333, New York, NY, USA, 2024. Association for Computing Machinery.

[2] Kaiyin Huang, Shaoyun Shi, and Wenlei Li. Integrability analysis of the Shimizu–Morioka system. *Communications in Nonlinear Science and Numerical Simulation*, 84:105101, 2020.

[3] T. Shimizu and N. Morioka. On the bifurcation of a symmetric limit cycle to an asymmetric one in a simple model. *Physics Letters A*, 76(3):201–204, 1980.

10.7 Solutions of Knizhnik-Zamolodchikov equation by dévissage

V. Hoang Ngoc Minh
University of Lille, France

In this work, solutions of universal differential equation (see (10.2) below, when the solutions exist) are provided using Volterra expansions for the Chen series. Ultimately, applied to the Knizhnik-Zamolodchikov (see (10.8) below) [1], this provides by *dévissage*[1] the unique grouplike solution satisfying asymptotic conditions. These solutions use a Picard-Vessiot theory of noncommutative differential equations and various factorizations of Chen series over the alphabet $\mathcal{T}_n := \{t_{i,j}\}_{1\leq i<j\leq n}$ and with coefficients in a commutative rings [2]. In particular, in the ring of holomorphic functions, $(\mathcal{H}(\mathcal{V}), 1_{\mathcal{H}(\mathcal{V})})$, over the simply connected differentiable manifold of $\mathbb{C}^n$, $\mathcal{V}$, the coefficients $\{\langle S \mid w\rangle\}_{w\in\mathcal{T}_n^*}$ of S are holomorphic and $\{\partial_i\langle S \mid w\rangle\}_{1\leq i\leq n}$ are well defined. So is the differential $d\langle S \mid w\rangle = \partial_1\langle S \mid w\rangle dz_1 + \cdots + \partial_n\langle S \mid w\rangle dz_n$. Thus, $\mathbf{d}$ can be defined over $\mathcal{H}(\mathcal{V})\langle\langle\mathcal{T}_n\rangle\rangle$ by

$$S = \sum_{w\in\mathcal{T}_n^*}\langle S \mid w\rangle w, \qquad \mathbf{d}S = \sum_{w\in\mathcal{T}_n^*}(d\langle S \mid w\rangle)w, \tag{10.1}$$

leading to the following noncommutative differential equation over $\mathcal{H}(\mathcal{V})\langle\langle\mathcal{T}_n\rangle\rangle$,

$$\mathbf{d}S = M_nS, \quad \text{where} \quad M_n := \sum_{1\leq i<j\leq n}\omega_{i,j}t_{i,j} \in \mathcal{L}ie_{\Omega(\mathcal{V})}\langle\mathcal{T}_n\rangle. \tag{10.2}$$

In particular, to the partition $\mathcal{T}_n$, onto $\mathcal{T}_{n-1}$ and $T_n := \{t_{k,n}\}_{1\leq k\leq n-1}$, corresponds the split of M_n:

$$M_n = \bar{M}_n + M_{n-1}, \quad \text{where } M_{n-1} \in \mathcal{L}ie_{\Omega(\mathcal{V})}\langle\mathcal{T}_{n-1}\rangle \quad \text{and } \bar{M}_n := \sum_{k=1}^{n-1}\omega_{k,n}\ t_{k,n} \in \mathcal{L}ie_{\Omega(\mathcal{V})}\langle T_n\rangle \tag{10.3}$$

For $N = n(n-1)/2$, the forms $\{\omega_i\}_{1\leq i\leq N}$ and the alphabet $X := \{x_k\}_{1\leq j\leq N}$ in bijection with $\mathcal{T}_n$,

$$\mathbf{d}S = M_nS, \quad \text{where} \quad M_n := \sum_{i=1}^{N}\omega_ix_j \in \mathcal{L}ie_{\Omega(\mathcal{V})}\langle X\rangle, \tag{10.4}$$

$$M_n = \sum_{1\leq k\leq N}F_k\ x_k = \sum_{1\leq l\leq n}U_l\ dz_l, \quad \text{where} \quad F_k = \sum_{1\leq l\leq n}f_{l,k}\ dz_j \text{ and then } U_l = \sum_{1\leq k\leq N}f_{l,k}\ x_k. \tag{10.5}$$

For $S \neq 0$ in the integral ring $\mathcal{H}(\mathcal{V})\langle\langle\mathcal{T}_n\rangle\rangle$, if S satisfies (10.2) then, by (10.5), one might have

$$\mathbf{d}S = M_nS = \sum_{1\leq l\leq n}(\partial_lS)\ dz_l, \quad \text{with} \quad \partial_lS = U_lS. \tag{10.6}$$

Since $\partial_j\partial_iS = ((\partial_jU_i) + U_iU_j)S$ and $\partial_i\partial_jS = \partial_j\partial_iS$ then $((\partial_jU_i) - (\partial_iU_j) + [U_i, U_j])S = 0$ and then $\partial_iU_j - \partial_jU_i = [U_i, U_j]$, $1 \leq i, j \leq n$. Or equivalently, $\mathbf{d}M_n = M_n \wedge M_n$ inducing a Lie ideal of relators among $\{t_{i,j}\}_{1\leq i<j\leq n}$, $\mathcal{J}_n$, and (10.2) are solved over $\mathcal{H}(\mathcal{V})\langle\langle\mathcal{T}_n\rangle\rangle$ and then $\mathcal{H}(\mathcal{V})\langle\langle\mathcal{T}_n\rangle\rangle/\mathcal{J}_n$.

According to Drinfel'd, M_n is *flat* and (10.2) is *completely integrable* [1]. Solution of (10.2), when exists, can be computed by convergent Picard's iteration over the topological basis $\{w\}_{w\in\mathcal{T}_n^*}$, *i.e.*

$$F_0(\varsigma, z) = 1_{\mathcal{H}(\mathcal{V})}, \quad F_i(\varsigma, z) = F_{i-1}(\varsigma, z) + \int_{\varsigma}^{z}M_n(s)F_{i-1}(s), i \geq 1, \tag{10.7}$$

[1] *I.e.* solutions of KZ_n, for $n \geq 3$, are obtained using those of KZ_{n-1} and the generating series of hyperlogarithms

and the sequence $\{F_k\}_{k\geq 0}$ admits the limit, called Chen series of the holomorphic forms $\{\omega_{i,j}\}_{1\leq i<j\leq n}$ and along a path $\varsigma \rightsquigarrow z$ over $\mathcal{V}$, modulo $\mathcal{J}_n$, is viewed as the fundamental solution of (10.2).

More generally, by a Ree's theorem, Chen series is grouplike belonging to $e^{\mathcal{L}ie_{\mathcal{H}(\mathcal{V})}\langle\langle\mathcal{T}_n\rangle\rangle}$ and can be put in the MRS factorization form [2] and [4]. Moreover, since the rank of the module of solutions of (10.2) is at most equals 1 then, under the action of the Haussdorf group, *i.e.* $e^{\mathcal{L}ie_{\mathbb{C}}\langle\langle\mathcal{T}_n\rangle\rangle}$ playing the rôle of the differential Galois group of (10.2) [2].

From these, in practice, infinite solutions of (10.2) can be computed using convergent iterations of pointwise convergence over $\mathcal{H}(\mathcal{V})\langle\langle\mathcal{T}_n\rangle\rangle$ and then $\mathcal{H}(\mathcal{V})\langle\langle\mathcal{T}_n\rangle\rangle/\mathcal{J}_n$. A challenge is to explicitly and exactly compute these limits of convergent sequences of (not necessarily grouplike) series on the dual topological ring and over various corresponding dual topological bases.

Applying (10.2)–(10.3), substituting $t_{i,j}$ by $t_{i,j}/2\mathrm{i}\pi$ and specializing $\omega_{i,j}$ to $d\log(z_i - z_j)$ and then $\mathcal{V}$ to the universal covering of the configuration space of n points on the complex plane $\mathbb{C}^n_* := \{z = (z_1, \ldots, z_n) \in \mathbb{C}^n | z_i \neq z_j \text{ for } i \neq j\}$, denoted by $\widetilde{\mathbb{C}^n_*}$, various expansions of Chen series over $\mathcal{H}(\widetilde{\mathbb{C}^n_*})\langle\langle\mathcal{T}_n\rangle\rangle$ provide solutions of the differential equation $\mathbf{d}F = \Omega_n F$, so-called KZ_n equation and Ω_n is so-called universal KZ connection form, defined by

$$\Omega_n(z) := \sum_{1\leq i<j\leq n} \frac{t_{i,j}}{2\mathrm{i}\pi} d\log(z_i - z_j) = \bar{\Omega}_n + \Omega_{n-1}, \quad \text{where} \quad \bar{\Omega}_n(z) := \sum_{k=1}^{n-1} \frac{t_{k,n}}{2\mathrm{i}\pi} d\log(z_k - z_n) \tag{10.8}$$

In particular, let $\Sigma_{n-2} = \{z_1, \ldots, z_{n-2}\} \cup \{0\}$ (for $z_{n-1} = 0$) be the set of singularities and $s = z_n$. For $z_n \to z_{n-1}$, the connection $\bar{\Omega}_n$ behaves as $(2\mathrm{i}\pi)^{-1}N_{n-1}$, where N_{n-1} is nothing but the connection of the differential equation satisfied by the noncommutative generating series of hyperlogarithms

$$N_{n-1}(s) := t_{n-1,n}\frac{ds}{s} - \sum_{k=1}^{n-2} t_{k,n}\frac{ds}{z_k - s} \in \mathcal{L}ie_{\Omega(\widetilde{\mathbb{C}\setminus\Sigma_{n-2}})}\langle T_n\rangle. \tag{10.9}$$

Let α^z_ς be the function on $\mathcal{T}^*_n$, mapping words to iterated integrals over the holomorphic 1-forms $\{d\log(z_i - z_j)\}_{1\leq i<j\leq n}$ along the path $\varsigma \rightsquigarrow z$ over $\widetilde{\mathbb{C}^n_*}$. The Chen series of $\{d\log(z_i - z_j)\}_{1\leq i<j\leq n}$ can be used to determine solutions of (10.8) and depends on the differences $\{z_i - z_j\}_{1\leq i<j\leq n}$. Furthermore, the universal KZ connection form Ω_n satisfies $\mathbf{d}\Omega_n - \Omega_n \wedge \Omega_n = 0$, inducing the relators associated to following relations on $\{t_{i,j}\}_{1\leq i<j\leq n}$ and generating the Lie ideal $\mathcal{J}_{\mathcal{R}_n}$ of $\mathcal{L}ie_{\mathcal{H}(\mathcal{V})}\langle\mathcal{T}_n\rangle$,

$$\mathcal{R}_n = \begin{cases} [t_{i,k} + t_{j,k}, t_{i,j}] = 0 & \text{for distinct } i,j,k, \quad 1 \leq i < j < k \leq n, \\ [t_{i,j} + t_{i,k}, t_{j,k}] = 0 & \text{for distinct } i,j,k, \quad 1 \leq i < j < k \leq n, \\ [t_{i,j}, t_{k,l}] = 0 & \text{for distinct } i,j,k,l, \quad \begin{cases} 1 \leq i < j \leq n, \\ 1 \leq k < l \leq n. \end{cases} \end{cases} \tag{10.10}$$

Then solutions of (10.8) are expected in $\mathcal{H}(\widetilde{\mathbb{C}^n_*})\langle\langle\mathcal{T}_n\rangle\rangle/\mathcal{J}_{\mathcal{R}_n}$.

For $z_n \to z_{n-1}$, grouplike solutions of (10.8) are of the form $h(z_n)H(z_1, \ldots, z_{n-1})$, where h satisfies the differential equation $df = (2\mathrm{i}\pi)^{-1}N_{n-1}f$ such that $h(z_n) \sim_{z_n\to z_{n-1}} (z_{n-1} - z_n)^{t_{n-1,n}/2\mathrm{i}\pi}$ and H satisfies the following differential equation

$$\mathbf{d}S = \Omega^{\phi_n}_{n-1}S, \quad \text{where} \quad \Omega^{\phi_n}_{n-1}(z) = \sum_{1\leq i<j\leq n-1} d\log(z_i - z_j)\phi_n^{(z^0,z)}(t_{i,j})/2\mathrm{i}\pi \tag{10.11}$$

and $\phi_n^{(z^0,z)}(t_{i,j}) \sim_{z_n\to z_{n-1}} e^{\mathrm{ad}_{-\log(z_{n-1}-z_n)t_{n-1,n}/2\mathrm{i}\pi}t_{i,j}} \mod \mathcal{J}_n$.

Let $\mathcal{D}_{\mathcal{T}_n}$ (resp. $\mathcal{D}_{T_n}$) denote the diagonal series on the $\sqcup\!\sqcup$-bialgebra $(\mathbb{Q}\langle\mathcal{T}_n\rangle, \mathtt{conc}, 1_{\mathcal{T}_n^*}, \Delta_{\sqcup\!\sqcup})$ (resp. $(\mathbb{Q}\langle T_n\rangle, \mathtt{conc}, 1_{T_n^*}, \Delta_{\sqcup\!\sqcup})$) endowed the dual bases $\{P_l\}_{l\in\mathcal{L}yn\mathcal{T}_n}$ and $\{S_l\}_{l\in\mathcal{L}yn\mathcal{T}_n}$ (resp. $\{P_l\}_{l\in\mathcal{L}yn T_n}$ and $\{S_l\}_{l\in\mathcal{L}yn T_n}$) indexed by Lyndon words on $\mathcal{L}yn\mathcal{T}_n$ (resp. $\mathcal{L}yn T_n$) [4]. Then solutions of (10.8) can be computed by the following recursion

$$V_k(\varsigma, z) = V_0(\varsigma, z) \sum_{t_{i,j}\in\mathcal{T}_{n-1}} \int_\varsigma^z \omega_{i,j}(s) S_0^{-1}(\varsigma, s) t_{i,j} V_{k-1}(\varsigma, s) \tag{10.12}$$

with $V_0(\varsigma, z) = (\alpha_\varsigma^z \otimes \mathrm{Id})\mathcal{D}_{T_n}$, or with $V_0(\varsigma, z) = (\alpha_\varsigma^z \otimes \mathrm{Id})\mathcal{D}_{T_n} \mod [\mathcal{L}ie_{\mathcal{H}(\mathcal{V})}\langle\langle T_n\rangle\rangle, \mathcal{L}ie_{\mathcal{H}(\mathcal{V})}\langle\langle T_n\rangle\rangle]$. Finally, there effectively exists $\{F_{S_l}\}_{l\in\mathcal{L}yn\mathcal{T}_n}$ such that the sequence $\{V_k\}_{k\geq 0}$ in (10.12) converges, in the first case, to the unique solution of (10.8) satisfying asymptotic conditions and achieving the *dévissage*:

$$\mathbb{F}_{KZ_n} = \prod_{l\in\mathcal{L}yn T_n}^{\searrow} e^{F_{S_l}P_l} \underbrace{\Big(1_{\mathcal{T}_n^*} + \sum_{v_1,\ldots,v_k\in T_n^*, t_1,\ldots,t_k\in\mathcal{T}_{n-1}, k\geq 1} F_{a(v_1t_1)\,\overline{\sqcup\!\sqcup}_2\ldots\overline{\sqcup\!\sqcup}_2\,a(v_kt_k)} r(v_1t_1)\ldots r(v_kt_k)\Big)}_{\text{functional expansion of solution of } KZ_{n-1}} \tag{10.13}$$

$$= \prod_{l\in\mathcal{L}yn\mathcal{T}_{n-1}}^{\searrow} e^{F_{S_l}P_l} \Big(\prod_{l=l_1l_2, l_2\in\mathcal{L}yn\mathcal{T}_{n-1}, l_1\in\mathcal{L}yn T_n}^{\searrow} e^{F_{S_l}P_l} \Big) \prod_{l\in\mathcal{L}yn T_n}^{\searrow} e^{F_{S_l}P_l} \tag{10.14}$$

while in the second case, it leads to an approximation of (10.13):

$$\mathbb{F}_{KZ_n} \equiv e^{\sum_{t\in T_n} F_t t} \Big(1_{\mathcal{T}_n^*} + \sum_{v_1,\ldots,v_k\in T_n^*, t_1,\ldots,t_k\in\mathcal{T}_{n-1}, k\geq 1} F_{a(\hat{v}_1t_1)\,\overline{\sqcup\!\sqcup}_2(\ldots\overline{\sqcup\!\sqcup}_2(a(\hat{v}_kt_k))\ldots)} r(v_1t_1)\ldots r(v_kt_k)\Big), \tag{10.15}$$

where $\overline{\sqcup\!\sqcup}_2$ denotes the half-shuffle product [3] and, for any $w = t_1\ldots t_m \in \mathcal{T}_n^*$,

$$a(w) = (-1)^m t_m\ldots t_1, \quad r(w) = \mathrm{ad}_{t_1}\circ\cdots\circ\mathrm{ad}_{t_{m-1}}\, t_m, \quad \hat{w} = t_1 \sqcup\!\sqcup \ldots \sqcup\!\sqcup\, t_m. \tag{10.16}$$

References

[1] V. Drinfel'd– *On quasitriangular quasi-Hopf algebras and on a group that is closely connected with Gal($\bar{\mathbb{Q}}/\mathbb{Q}$)*, *Leningrad Math. J.*, 4, 829-860, 1991.

[2] G. Duchamp, V. Hoang Ngoc Minh, V. Nguyen Dinh.– *Towards a noncommutative Picard-Vessiot theory*, In preparation. arXiv:2008.10872

[3] Loday, J-L.– *Cup-product for Leibniz cohomology and dual Leibniz algebras*, Math. Scand., 77 (1995), no. 2, pp. 189-196.

[4] Reutenauer C.– *Free Lie Algebras*, London Math. Soc. Monographs (1993).

10.8 Recent Advancements in Noncommutative Gröbner Basis Software

Clemens Hofstadler
Johannes Kepler University, Austria

In recent years, noncommutative Gröbner bases in free algebras (also known as Gröbner-Shirshov bases) have found important applications in areas such as (linear) control theory [9],

automated theorem proving for operator statements [3], [4], [10] and [12], as well as in graph [11] and game theory [8].

These applications crucially rely on the ability to compute Gröbner bases in free algebras efficiently. While software for commutative Gröbner basis computations has seen remarkable progress in recent years (see [1] and references therein), noncommutative tools seem to lag behind. They often lack the same level of efficiency and sophistication, and mostly rely on outdated algorithms and data structures.

In this talk, we give an overview of existing software for Gröbner basis computations in free algebras. We also present `f4ncgb` [5], a new open-source C++ library for this task. Moreover, we discuss recent algorithmic improvements that could be integrated into existing tools in the future, in particular, signature-based algorithms [2] and [6] and support for more general coefficient domains such as the integers [7].

References

[1] J. Berthomieu, C. Eder, and M. Safey El Din. msolve: A Library for Solving Polynomial Systems. In *Proceedings of ISSAC 2021*, pp. 51–58, 2021.

[2] C. Eder and J.C. Faugère. A survey on signature-based algorithms for computing Gröbner bases. *Journal of Symbolic Computation*, 80:719–784, 2017.

[3] C. Hofstadler. *Noncommutative Gröbner bases and automated proofs of operator statements*. PhD thesis, Johannes Kepler University Linz, Austria, 2023. Available at `https://resolver.obvsg.at/urn:nbn:at:at-ubl:1-67821`.

[4] C. Hofstadler, C.G. Raab, and G. Regensburger. Universal truth of operator statements via ideal membership. *arXiv preprint*, arXiv:2212.11662, 2022.

[5] M. Heisinger and C. Hofstadler. f4ncgb: High Performance Gröbner Basis Computations in Free Algebras. *arXiv preprint*, arXiv:2505.19304, 2025.

[6] C. Hofstadler and T. Verron. Signature Gröbner bases, bases of syzygies and cofactor reconstruction in the free algebra. *Journal of Symbolic Computation*, 113: 211–241, 2022.

[7] V. Levandovskyy, T. Metzlaff, and K. Abou Zeid. Computation of free non-commutative Gröbner bases over $\mathbb{Z}$ with Singular:Letterplace. In *Proceedings of ISSAC 2020*, pp. 312–319, 2020.

[8] S. Yan, J. Yang, T. Yu, and L. Zhi. A Characterization of Perfect Strategies for Mirror Games. In *Proceedings of ISSAC 2023*, pp. 545–554, 2023.

[9] J.W. Helton, M. Stankus, and J.J. Wavrik. Computer simplification of formulas in linear systems theory. *IEEE Transactions on Automatic Control*, 43(3):302–314, 1998.

[10] J.W. Helton and J.J. Wavrik. Rules for computer simplification of the formulas in operator model theory and linear systems. In *Nonselfadjoint operators and related topics*, pp. 325–354, 1994.

[11] V. Levandovskyy, C. Eder, A. Steenpass, S. Schmidt, J. Schanz, and M. Weber. Existence of Quantum Symmetries for Graphs on Up to Seven Vertices: A Computer based Approach. In *Proceedings of ISSAC 2022*, pp. 311–318, 2022.

[12] L. Schmitz and V. Levandovskyy. Formally verifying proofs for algebraic identities of matrices. In *Proceedings of CICM 2020*, pp. 222–236, 2020.

10.9 Computing centralizers for linear differential operators

Antonio Jiménez-Pastor
Universidad Politécnica de Madrid, Spain

In this talk we are going to present our recent work [2]. In this work, we are devoted on the computation and the study of the centralizer of a linear ordinary differential operator Z(L), i.e., the set of linear differential operators that commute with the given operator L. When the centralizer is non-trivial, it is a known result that Z(L) is the coordinate ring of a spectral curve.

Based on Goodearl's structural result [1] and the concept of almost commuting operators [3], we provide a new algorithm to compute a filtered basis of the centralizer Z(L) as a C[L]-module for solutions of the stationary Gelfand-Dickey hierarchies. We also provide a family of examples for solutions of these hierarchies for operators of order 3, 4 and 5.

All results are implemented in the computer algebra system SageMath [4], within the package dalgebra.

This is a joint work with Sonia L. Rueda.

References

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

[2] Jiménez-Pastor, A., Rueda, S. L. Effective computation of centralizers of ODOs. *Preprint, arXiv:2505.01289* (2025).

[3] Jiménez-Pastor, A., Rueda, S. L., Zurro, M. A., Heredero, R. H., and Delgado, R. Computing Almost Commuting Bases of ODOs and Gelfand-Dickey Hierarchies. *Math.Comput.Sci. 19*, 1 (2025).

[4] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 10.5)*, 2024. `https://www.sagemath.org`.

10.10 Undecidability of Noncommutative Ideal Membership and Counterexamples of Operator Statements

Peter Krug[1], Georg Regensburger[1] and Clemens Hofstadler[2]

[1] University of Kassel, Germany

[2] Johannes Kepler University, Austria

Computations with identities of linear operators can be translated into symbolic computations with noncommutative polynomials in free algebras. Through this translation, proving the correctness of operator identities reduces to verifying ideal membership of such polynomials [4] and [5]. While verifying ideal membership in free algebras is always possible using noncommutative Gröbner bases, disproving it is in general undecidable [6]. Nevertheless, in practice, one can often refute ideal membership by constructing explicit counterexamples (in the form of matrices).

In this talk, we first outline the undecidability of the ideal membership problem in free algebras. While one would think that ideals with undecidable membership problem are monstrous, complicated objects, already Tseitin [2] and [7] provided a simple example of such an ideal, which we discuss in the talk. We also present a method to compute explicit matrix counterexamples by combining SAT solving and algebraic techniques (Hensel lifting and rational reconstruction). As a special case, we discuss how to compute simple counterexamples containing only 0 and ± 1 as entries. These methods are implemented in SageMath as part of the operator_gb package [1]. We illustrate them on examples coming from the theory of generalized inverses [3].

References

[1] K. Bernauer, C. Hofstadler, and G. Regensburger. How to Automatise Proofs of Operator Statements: Moore–Penrose Inverse; A Case Study. In *Proceedings of CASC 2023*, pp. 39–68, 2023.

[2] D.J. Collins. A simple presentation of a group with unsolvable word problem. In *Illinois Journal of Mathematics*, 30(2): 230–234, 1986.

[3] D.S. Cvetković-Ilić, C. Hofstadler, J. Hossein Poor, J. Milošević, C.G. Raab, and G. Regensburger. Algebraic proof methods for identities of matrices and operators: improvements of Hartwig's triple reverse order law. In *Applied Mathematics and Computation*, 409:126357, 2021.

[4] C. Hofstadler. *Noncommutative Gröbner bases and automated proofs of operator statements.* PhD thesis, Johannes Kepler University Linz, Austria, 2023. Available at `https://resolver.obvsg.at/urn:nbn:at:at-ubl:1-67821`.
[5] C. Hofstadler, C.G. Raab, and G. Regensburger. Universal truth of operator statements via ideal membership. *arXiv preprint*, arXiv:2212.11662, 2022.
[6] T. Mora. An introduction to commutative and noncommutative Gröbner bases. In *Theoretical Computer Science*, 134(1):131–173, 1994.
[7] G.S. Tseitin. An associative calculus with an insoluble problem of equivalence. In *Trudy Matematicheskogo Instituta imeni VA Steklova*, 52:172–189, 1958 (in russian).

10.11 Generalized Gröbner Bases and Dimension Polynomials of D-modules

Alexander Levin
The Catholic University of America, Washington, DC, USA

We consider several term orderings in a finitely generated free module E over a Weyl algebra $A_n(K)$ that are associated with a partition of the basic set of variables of $A_n(K)$. Using these term orderings, we introduce a new type of reductions in the module E and Gröbner-type bases associated with these reductions. Properties of the introduced bases allow us to obtain a multivariate dimension polynomial of a finitely generated D-module, that is, a left $A_n(K)$-module. We present invariants of such dimension polynomials and prove an intersection property for multivariate filtrations in a certain class of D-modules. The obtained results generalize theorems on bivariate Bernstein-type dimension polynomials proved in [1] and reveal new characteristics of finitely generated D-modules.

References

[1] C. Dönch; A. Levin. Bivariate Dimension Polynomials and New Invariants of Finitely Generated D-Modules. *Int. J. Algebra Comput.*, 23: 1625–1651, 2013.

10.12 Combining Sparsity and Symmetry Exploitation for SOS-Certificates

Tobias Metzlaff
LAAS-CNRS, France

Based on joint work with I. Klep (Ljubljana), V. Magron (Toulouse) and J. Wang (Beijing) and supported by QuantERA II ERA-NET European Union's Horizon 2020 research and innovation programme COMPUTE.

SOS-Certificates

Let A be a graded real *-algebra. Given $f \in A$, a sums-of-squares (SOS) certificate is a representation of f in the form

$$f = \sum_t q_t\, q_t^*$$

with finitely many $q_t \in A$.

As a historical motivation, we take Hilbert's proof from 1888 that every nonnegative homogeneous polynomial $f \in A = \mathbb{R}[X] = \mathbb{R}[X_1, \ldots, X_n]$ (with * the identity) of degree $2r$ can be written as a sum of squares if and only if $(n, 2r) \in \{(2, 2r), (n, 2), (3, 4)\}$. The first example however of a nonnegative polynomial which is not a sum of squares was given later in 1967 by Motzkin, indicating that it is far from trivial to find an explicit SOS-certificate (or to disprove its existence).

Theorems that state the existence of an SOS-certificate are called Positivstellensätze, see for example [7] and [9], and enable solving computational problems with techniques from real algebra geometry [3] and [10]. Some applications are polynomial optimization

$$\begin{array}{rcccll} f^* = & \min & f(X) & \geq & \max & \lambda \\ & \text{s.t.} & X \in \mathbb{R}^n & & \text{s.t.} & \lambda \in \mathbb{R}, \\ & & & & & f - \lambda \text{ is SOS in } \mathbb{R}[X] \end{array} \tag{POP}$$

with $f \in \mathbb{R}[X]$, see [2], computing a maximal positive invariant set of a dynamical system $\dot{X}(t) = \mathbf{f}(X(t))$, see [1], or verifying Kazhdan's property (T) for a finitely generated group $\mathfrak{G}$, which holds if and only if

$$\Delta^2 - \lambda\,\Delta \text{ is SOS in } \mathbb{R}[\mathfrak{G}] \tag{T}$$

for some $\lambda > 0$ with Laplacian Δ, see [6].

Computing an explicit SOS representation can give not only the solution to the problem but also an optimizer in which the solution is attained. In practice, this often boils down to solving a semidefinite program (SDP), which is obtained by restricting the degrees of the sums of squares and constructing a hierarchy of numerical bounds up to a satisfying precision. Naturally, these problems become very difficult to handle computationally and tools to gain efficiency whilst preserving numerical accuracy are required.

Symmetry Reduction

Let G be a finite group acting on the algebra A and its subspaces A_r of degree at most r, which are assumed to be finite dimensional. As a vector space, each A_r (or more precisely its complexification) has an isotypic decomposition

$$A_r = \bigoplus_{i=1}^{h} \bigoplus_{j=1}^{m_r^{(i)}} V_j^{(i)},$$

where h is the number of irreducible characters of G and $m_r^{(i)}$ are their multiplicities [11]. A vector space basis admitting this decomposition is called symmetry-adapted. By Schur's Lemma, we may choose a total of $m_r^{(i)}$ distinguished basis elements from the i–th component and denote them by $w_j^{(i)} \in V_j^{(i)}$.

Let $f \in A$ be a G-invariant objective function of degree $2\,r_{\min}$ for which we seek an SOS-certificate in A and denote by $\mathcal{R}^G$ the Reynolds operator. For $r \geq r_{\min}$, we approximate f as

$$f = \sum_{i=1}^{h} \mathcal{R}^G(q_r^{(i)}) \quad \text{with sums of squares} \quad q_r^{(i)} = (\mathbf{w}_r^{(i)})^t \cdot \mathbf{Q}_r^{(i)} \cdot (\mathbf{w}_r^{(i)})^*.$$

Here, $\mathbf{w}_r^{(i)}$ is the vector of basis elements $w_j^{(i)}$, $1 \leq j \leq m_r^{(i)}$, and $\mathbf{Q}_r^{(i)}$ is a Hermitian positive semidefinite matrix, that is, $q_r^{(i)}$ is a sum of squares in the vector space generated by the $w_j^{(i)}$, see [4] and [8].

Adding Term Sparsity

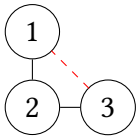
The term sparsity pattern (tsp) is encoded by a graph with nodes given by a basis for A_r. Without going into the technical details of the construction of the edges, one can follow [12] to construct a sequence of binary matrices

$$\mathbf{B}_{r,s}^{(i)} \subseteq \mathbf{B}_{r,s+1}^{(i)} \subseteq \mathbf{B}_{r,s+2}^{(i)} \subseteq \ldots \in \{0,1\}^{m_r^{(i)} \times m_r^{(i)}},$$

such that one only considers sums of squares with term sparsity (TSSOS) of the form

$$q_{r,s}^{(i)} = (\mathbf{w}_r^{(i)})^t \cdot (\mathbf{B}_{r,s}^{(i)} \circ \mathbf{Q}_r^{(i)}) \cdot (\mathbf{w}_r^{(i)})^*.$$

Here, $\circ$ denotes the Hadamard product and s is the sparse order. For example, the graph



is represented by the binary matrix $\mathbf{B} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}$

and encodes that basis elements $\mathfrak{b}_1$, $\mathfrak{b}_2$, $\mathfrak{b}_3$ appear in the problem data as $\mathfrak{b}_1\,\mathfrak{b}_2$ or $\mathfrak{b}_2\,\mathfrak{b}_3$, but not $\mathfrak{b}_1\,\mathfrak{b}_3$.

Symmetric TSSOS Hierarchy

For POP, we obtain a semidefinite lower bound

$$\begin{aligned} f^* \geq f_{\text{sos}}^{r,s} := \quad & \max \quad \lambda \\ & \text{s.t.} \quad \lambda \in \mathbb{R}, \\ & \qquad f - \lambda \in \text{SOS}^G(\mathbf{B}_{r,s}^{(1)}) \oplus \ldots \oplus \text{SOS}^G(\mathbf{B}_{r,s}^{(h)}), \end{aligned}$$

where $\text{SOS}^G(\mathbf{B}_{r,s}^{(i)})$ is the convex cone of sparse G-invariant sums of squares $\mathcal{R}^G(q_{r,s}^{(i)})$.

Theorem. *For fixed $r \geq r_{\min}$, the sequence $(f_{\text{sos}}^{r,s})_{s\geq 1}$ is monotonously nondecreasing and converges in finitely many steps to some $f_{\text{sos}}^{r,*} \leq f^*$. For fixed $s \geq 1$, the sequence $(f_{\text{sos}}^{r,s})_{r\geq r_{\min}}$ is monotonously nondecreasing. Under additional algebraic assumptions and constraints, one has asymptotic convergence $f_{\text{sos}}^{\infty,*} = f^*$.*

Conclusion, Work in Progress, Outlook

By symmetry reduction, a matrix representation of a sum of squares is not of size $\dim(A_r)^2$, but splits into potentially much smaller blocks $\mathbf{Q}_r^{(i)}$ of combined size $(m_r^{(1)})^2 + \ldots + (m_r^{(h)})^2$. By sparsity exploitation, one removes further entries of these matrices according to tsp graphs.

The preprocess of achieving such a reduction involves the computation of a symmetry adapted basis. However, this basis does not depend on the specific form of the objective function, but only on the group G and the degree r. Hence, one such preprocess can be reapplied for multiple problems. Afterwards, computing the reduced SDP is more efficient than the original one.

In the talk, I will quantify these computational gains via benchmarks on a selection of polynomial optimization problems, for which we used the Julia package TSSOS:

https://github.com/wangjie212/TSSOS

We are currently working on the combination of symmetry with further sparsity types, see [5], and on the generalization of the above convergence result to noncommutative algebras.

References

[1] M. Korda, D. Henrion, and C. Jones. Convex Computation of the Maximum Controlled Invariant Set For Polynomial Control Systems. *SIAM Journal on Control and Optimization*, 52(5):10.1137/130914565, 2013.

[2] J.-B. Lasserre. Global Optimization with Polynomials and the Problem of Moments. *SIAM Journal on Optimization*, 11(3):796–817, 2001.

[3] M. Marshall. *Positive polynomials and sums of squares.* Number 146 in Mathematical Surveys and Monographs. American Mathematical Society, 2008.

[4] T. Metzlaff. On symmetry adapted bases in trigonometric optimization. *Journal of Symbolic Computation*, 127(102369), 2025.

[5] V. Magron and J. Wang. *Sparse Polynomial Optimization - Theory and Practice.* Series on Optimization and Its Applications: Volume 5. World Scientific, Europe, 2023.

[6] N. Ozawa. Noncommutative real algebraic geometry of Kazhdan's property (T). *Journal of the Institute of Mathematics of Jussieu*, 15(1):85–90, 2016.

[7] M. Putinar. Positive polynomials on compact semi–algebraic sets. *Indiana University Mathematics Journal*, 42(3):969–984, 1993.

[8] C. Riener, T. Theobald, L. Andrén, and J.-B. Lasserre. Exploiting Symmetries in SDP-Relaxations for Polynomial Optimization. *Mathematics of Operations Research*, 38(1):122–141, 2013.

[9] K. Schmüdgen. The K-moment problem for compact semi-algebraic sets. *Mathematische Annalen*, 289(1):203–206, 1991.

[10] K. Schmüdgen. *Noncommutative Real Algebraic Geometry - Some Basic Concepts and First Ideas*, pages 325–350. Springer New York, New York, NY, 2009.

[11] J.-P. Serre. *Linear Representations of Finite Groups.* Graduate Texts in Mathematics. Springer, New York, 1977.

[12] J. Wang, V. Magron, and J.-B. Lasserre. TSSOS: a moment-SOS hierarchy that exploits term sparsity. *SIAM Journal on Optimization*, 31(1):30–58, 2021.

10.13 New algorithm for differential elimination based on support bound

Yulia Mukhina
École Polytechnique, Institute Polytechnique de Paris, France

Differential elimination refers to finding consequences of a system of differential equations depending only on a chosen subset of variables. In the context of dynamical modeling, one often starts with a polynomial dynamical system of the form $\mathbf{x}' = \mathbf{g}(\mathbf{x})$ and is interested to obtain the minimal equation satisfied by a single component of $\mathbf{x}$ (for example, x_1). Based on the degrees of the polynomials in $\mathbf{g}$, we give an upper bound on the support of such minimal equation which can be further used, for example, for computing this equations using an ansatz. We show that our bound is sharp in "more than half the cases"

10.14 Closed forms of power series with hypergeometric-type terms

Bertrand Teguia Tabuguia
University of Oxford, UK

This talk focuses on power series representations of univariate D-finite and D-algebraic functions whose general coefficients linearly involve hypergeometric terms. For D-finite functions, we present an algorithmic improvement over [8] designed to further simplify outputs not in normal

forms. For D-algebraic (and non-D-finite) functions, we detail an ongoing investigation into detecting closed forms represented as linear polynomials in $\mathcal{H}[S(n)]$, where $\mathcal{H}$ is the ring of hypergeometric-type terms, and $S(n)$ is the nth term of Bernoulli or Euler numbers. The presentation is structured into these two distinct parts.

Simplifying FPS outputs

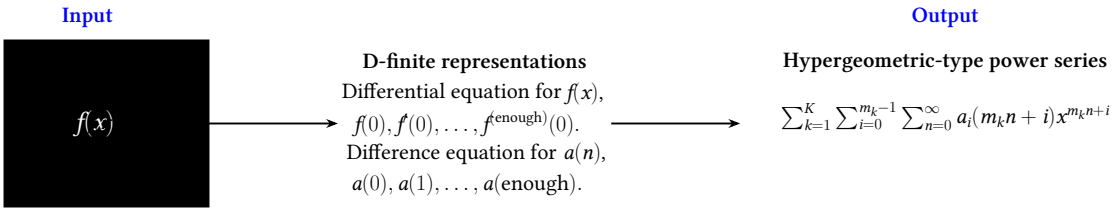


Figure 10.1: The FPS algorithm for hypergeometric-type power series.

Drawing from [5] and [6], this part of the talk will introduce the computable ring of hypergeometric-type sequences $(\mathcal{H})$ and showcase its properties using our Maple package. Figure 10.1 provides a high-level overview of the FPS algorithm, with arrows indicating its key steps. This algorithm is designed to take a black-box mathematical expression and first construct a D-finite representation. If successful, it solves the corresponding D-finite recurrence for m-fold hypergeometric term solutions, ultimately constructing the power series as an appropriate linear combination of these terms.

Sometimes, the order of the obtained recurrence equation is too small to enable the algorithm to escape unnecessary splitting fields. The generating function $f(x) := \frac{x\left(-x^4+7x^3+6x^2+7x+5\right)}{(1-x)^4(x^2+x+1)}$ of the OEIS sequence A208946 is a typical example. The FPS algorithm internally solves a 7th-order recurrence equation and returns

$$\texttt{FPS}(f(x), x, n) = \sum_{n=0}^{\infty} \left(-\frac{2\cos\left(\frac{2n\pi}{3}\right)}{3} - \frac{2\sqrt{3}\,\sin\left(\frac{2n\pi}{3}\right)}{9} + \frac{4n^3}{3} + 2n^2 + n + \frac{2}{3} \right) x^n. \tag{10.17}$$

An equivalent result is obtained with the Maple command `convert/FormalPowerSeries`, which implements a variant of FPS. Using our software from [5], we compute the normal form

$$\texttt{HyperTypeSeq} : -\texttt{HTS}\left(-\frac{2\cos\left(\frac{2n\pi}{3}\right)}{3} - \frac{2\sqrt{3}\,\sin\left(\frac{2n\pi}{3}\right)}{9}, n \right) = -\frac{2\chi_{\{modp(n,3)=0\}}}{3} + \frac{2\chi_{\{modp(n,3)=2\}}}{3}. \tag{10.18}$$

By the correspondence between hypergeometric-type power series and hypergeometric-type terms, we deduce the simplified closed form below.

$$f(x) = \sum_{n=0}^{\infty} \left(\frac{4n^3}{3} + 2n^2 + n + \frac{2}{3} \right) x^n - \frac{2}{3} \sum_{n=0}^{\infty} x^{3n} + \frac{2}{3} \sum_{n=0}^{\infty} x^{3n+2}. \tag{10.19}$$

D-algebraic series solutions of quadratic ODEs

We aim to consider D-algebraic power series whose general coefficients have the closed form:

$$\alpha(n) + \beta(n)\, S(n), \tag{10.20}$$

where $\alpha(n), \beta(n) \in \mathcal{H}$, and $(S(n))$ is a non-D-finite sequence which has the zero sequence as a subsequence. The target algorithm assumes that $S(n)$ is known. For example, $S(n)$ could be the nth Bernoulli number B_n, which has the following properties.

$$B_0 = 1,\ B_{2n} = \frac{(-1)^{n+1} 2\,(2n)!}{(2\pi)^{2n}} \zeta(2n),\ n \geq 1, \tag{10.21}$$

$$B_{2n+1} = 0,\ n \geq 1. \tag{10.22}$$

In (10.21), ζ is the Riemann Zeta function. Such a formula is not supposed to be known; what the algorithm requires is the ability to (efficiently) compute terms of $S(n)$ (B_n in this case). We aim to recover closed forms of power series involving numbers such as Bernoulli and Euler numbers, and potentially discover hidden formulae in the form of (10.20). At present, we are investigating proofs for the correctness of the results. Indeed, the algorithm combines D-finite and D-algebraic guessing (see [2] to [4]) together with the hypergeometric-type representation algorithm from [5] and [6].

A simple situation corresponds to when $\alpha(n) = 0$ in (10.20). In [7], we proposed an approach to extend the FPS algorithm for non-D-finite functions that satisfy quadratic differential equations. For $f(x) := \tan(x)$, the algorithm uses the following differential equation to return a recursive formula for the series.

$$y''(x) - 2\, y(x)\, y'(x) = 0. \tag{10.23}$$

Using quadratic guessing [4], one can obtain the same equation from the first few coefficients of the power series of $f(x)$.

Assuming $f(x) = \sum_{n=0}^{\infty} a_n x^n$, we use D-finite guessing from [3] to construct a holonomic recurrence equation for $\frac{a_{2n-1}}{B_{2n}}$, $n \geq 1$. Using the guessed recurrence and the initial values we detect the identity

$$a_n = \frac{(-1)^{\frac{n}{2}-\frac{1}{2}}\, 2^{n+1}\, (2^{n+1}-1)}{(n+1)\,!}\, \chi_{\{n \equiv 1 \mod 2\}} B_{2n},\ n \geq 1, \tag{10.24}$$

where $\chi_{\{n \equiv 1 \mod 2\}}$ is our mathematical notation of interlacement, implemented in Maple with the notation given in (10.18). The final step is to use quadratic guessing to construct (10.23) from the first terms of the right-hand side in (10.24) and verify that $f(x)$ satisfies it. This is indeed successful, and we deduce the classical formula for the tangent power series.

$$f(x) = \sum_{n=0}^{\infty} \frac{(-1)^n 4^{n+1} (4^{n+1}-1) B_{2(n+1)}}{(2(n+1))!} x^{2n+1}. \tag{10.25}$$

When $\alpha(n) \neq 0$, we investigate shape lemmas related to Ritt factorizations of differential polynomials. Our goal is to construct a specific type of algebraic differential equations satisfied by sums of D-finite and D-algebraic (and not D-finite) functions. This enables us to determine $\alpha(n)$ from the nonlinear recursion of $\alpha(n) + \beta(n)\, S(n)$ and the indices where $S(n) = 0$. A particular challenge arises when $\alpha(n)$ vanishes at the same indices as $S(n)$, making it difficult to pinpoint the initial terms of $\alpha(n)$. We mention the work of Gao and Zang [1] on the decomposition of differential polynomials, which could be relevant for our context and warrants further exploration.

Keywords: Hypergeometric-type terms, Bernoulli numbers, Euler numbers, quadratic differential equations, guessing.

Acknowledgment. The author is supported by UKRI Frontier Research Grant EP/X033813/1.

References

[1] Gao, X.S., Zhang, M.: Decomposition of differential polynomials with constant coefficients. In: Proceedings of the 2004 international symposium on Symbolic and algebraic computation. pp. 175–182 (2004)
[2] Kauers, M., Koutschan, C.: Guessing with little data. In: Proceedings of the 2022 International Symposium on Symbolic and Algebraic Computation. pp. 83–90 (2022)
[3] Salvy, B., Zimmermann, P.: GFUN: a Maple package for the manipulation of generating and holonomic functions in one variable. ACM Transactions on Mathematical Software (TOMS) **20**(2), 163–177 (1994)
[4] Teguia Tabuguia, B.: Guessing with quadratic differential equations. Software Demo at ISSAC'22. arXiv preprint arXiv:2207.01037 (2022)
[5] Teguia Tabuguia, B.: Computing with hypergeometric-type terms. ACM Communication in Computer Algebra **58**(2), 23 – 26 (2024)
[6] Teguia Tabuguia, B.: Hypergeometric-type sequences. Journal of Symbolic Computation **125**, 102328 (2024).
[7] Teguia Tabuguia, B., Koepf, W.: On the representation of non-holonomic univariate power series. Maple Transactions **2**(1) (2021)
[8] Teguia Tabuguia, B., Koepf, W.: Symbolic conversion of holonomic functions to hypergeometric type power series. Programming and Computer Software **48**(2), 125–146 (2022)

10.15 An algorithmic problem for Nijenhuis Lie algebras

Chia Zargeh
Modern College of Business & Science, Oman

In this work, we address an algoritmic problem for Nijenhuis Lie algebras. We introduce the concept of HNN-extension for Nijenhuis Lie algebras and employ the Gröbner-Shirshov basis theory for free Nijenhuis Lie algebras to provide an embedding theorem.

The role of the Nijenhuis operator on a Lie algebra has been used in the study of integrability of nonlinear evolution equations in [1]. In this work, we spread the concept of HNN-extension which is an important construction in combinatorial group theory to free Nijenhuis Lie algebras. HNN-extension has been spread to various algebraic structures such as Lie (super)algebras, Leibniz algebras, semigroups, and rings. The following presentation exists for HNN-extension of Lie algebra $\mathcal{L}$:

$$\mathcal{H} = \langle \mathcal{L}, t \mid [t, a] = d(a), \text{ for all } a \in \mathcal{A} \rangle, \tag{10.26}$$

where d is a derivation map defined on a subalgebra $\mathcal{A}$ and t is a new generating letter. We develop this construction to the case of free Nijenhuis Lie algebras. To this end, we recall the theory of Gröbner-Shirshov basis for Lie Ω-algebras introduced in [3] and provide a presentation for HNN-extension of free Nijehuis Lie algebras. As for an application of HNN-extension, we provide an embedding theorem. It is worth noting that HNN-extension provides alternative proofs for known embedding theorems, and used in undecidability of Markov properties (see [2] and references herein).

References

[1] I. Dorfman. Dirac Structures and Integrability of Nonlinear Evolution Equations. (Wiley, Chichester, 1993).
[2] A. Najafizadeh, C. Zargeh On the undecidability of Markov properties for Lie superalgebras. *J. Algebra Comb. Discrete Appl.* 12(1):43-52. 2025.

[3] J. Qiu, Y. Chen. Groebner-Shirshov bases for Lie Ω-algebras and free Rota-Baxter Lie algebras. *J. Alg. Appl.*, 16(2):1750190, 2017.

10.16 Faster multivariate integration in D-modules

Hadrien Brochet
Inria Saclay, France

Not all integrals can be expressed in closed form using elementary functions, as shown by Liouville's theorem. In contrast, the integral of a holonomic/D-finite function is always holonomic/D-finite, that is the integral of a function satisfying sufficiently many linear differential equations (LDEs) with polynomial coefficients also satisfies such a system of LDEs. This makes the holonomic and D-finite frameworks particularly relevant for symbolic integration.

I will address two central algorithmic problems in this field: the problem of integration with parameters, where one seeks a differential equation satisfied by a parametric integral, and the reduction problem, where the goal is to find linear relations between integrals. Two distinct approaches exist, the D-finite one and the holonomic one. The D-finite approach has been the most studied one and offers efficient algorithms, but it lacks the full expressivity of the holonomic setting, which can handle a broader class of integrals and particularly those over semi-algebraic sets. However, the current algorithms developed for the holonomic setting have a prohibitive computational cost. I will present a new reduction algorithm working in a mixed approach, aiming to balance the efficiency of D-finiteness with the expressivity of holonomy. This reduction is inspired by the Griffiths–Dwork method for rational functions [1] and [2] and yields similarly an algorithm for the problem of parametric integration.

As an application, I will present the computation of a differential equation for the generating function of 8-regular graphs, which was out of reach so far.

This work was conducted jointly with my PhD advisors, Frédéric Chyzak and Pierre Lairez, and is based on our paper [3].

References

[1] A. Bostan, P. Lairez, B. Salvy. Creative telescoping for rational functions using the Griffiths-Dwork method. Proceedings of the 38th International Symposium on Symbolic and Algebraic Computation, 93-100, 2013.
[2] P. Lairez. Computing periods of rational integrals. Mathematics of computation 85, pp. 1719-1752, 2016.
[3] H. Brochet, F. Chyzak, P. Lairez. Faster multivariate integration in D-modules. Preprint, 2025.

10.17 A Shape Lemma for Ideals of Differential Operators

Manuel Kauers
Johannes Kepler University, Austria

Joint work with Christoph Koutschan and Thibaut Verron.

We will report on a recent joint article with Koutschan and Verron (J. Algebra, 677:448–459, 2025) in which we propose a version of the classical shape lemma for zero-dimensional ideals of a commutative multivariate polynomial ring to the noncommutative setting of zero- dimensional ideals in an algebra of differential operators.

10.18 The Expansion Complexity of Ultimately Periodic Sequences over Finite Fields

Yi Zhang
Xi'an Jiaotong-Liverpool University, China

The expansion complexity is a new figure of merit for cryptographic sequences. In this paper, we present an explicit formula of the (irreducible) expansion complexity of ultimately periodic sequences over finite fields. We also provide improved upper and lower bounds on the N-th irreducible expansion complexity when they are not explicitly determined. In addition, for some infinite sequences with given nonlinear complexity, a tighter upper bound of their N-th expansion complexity is given. This a joint work with Zhimin Sun, Xiangyong Zeng, Chunlei Li, and Lin Yi.

SPECIAL SESSION 11

Sparse Interpolation and Technology

What is known as sparse interpolation in computer algebra, is called exponential analysis in digital signal processing. A basic algorithm to solve the former is the Ben-Or/Tiwari algorithm, while the latter problem is often reformulated as a matrix pencil problem. In the past 10 years, the cross fertilization of properties and algorithms has led to progress in both worlds.

In this special session we discuss some results obtained in real-life applications, as a result of the connection between sparse interpolation and exponential analysis. Among others we mention:

- Fluorescence Lifetime Imaging (FLIM) and Diffuse Correlation Spectroscopy (DCS) in biomedical engineering,
- Operational Deposit Modelling in finance,
- Uniform Linear Array sparsification and synthesis in antenna engineering,
- Superresolution and Validation in digital signal processing,
- Curve generation in Computer Aided Design (CAD),
- Modelling of key performance metrics for reflector antennas in radioastronomy.

Session organizers

- Wen-shin Lee (University of Stirling, Scotland, UK)
- Anthony O'Hare (University of Stirling, Scotland, UK)

11.1 Sparse Interpolation in CS&E

Annie Cuyt
University of Stirling, UK
University of Antwerp, Belgium

What is called Sparse Interpolation (SI) in computer algebra is termed Exponential Analysis (EA) in signal processing. The respective goal is to identify and reconstruct a sparse linear combination of monomials or a sparse linear combination of exponential functions.

We discuss how SI and EA can cross-fertilize and lead to new results in several Computational Science and Engineering problem statements. Among other things, we discuss antenna design [6], torsional vibration, radioastronomy metrics [7], financial time series analysis, fluorescence lifetime imaging [8], direction of arrival [3], localisation problems [4] and [5], texture analysis [2], radar imaging [1],...

References

[1] A. Cuyt, Y. Hou, F. Knaepkens, and W.-s. Lee. Sparse multidimensional exponential analysis with an application to radar imaging. SIAM J. Scient. Comp., 42:B675–B695, 2020.

[2] Y. Hou, A. Cuyt, W.-s. Lee, and D. Bhowmik. Decomposing textures using exponential analysis. In IEEE ICASSP 2021 Proceedings, 1920–1924, 2021.

[3] F. Knaepkens, A. Cuyt, W.-s. Lee, and D.I.L. de Villiers. Regular sparse array direction of arrival estimation in one dimension. IEEE Trans. Antennas Propag., 68:3997–4006, 2020.

[4] R. Louw, F. Knaepkens, A. Cuyt, W.-s. Lee, S. J. Wijnholds, D.I.L. de Villiers, and R.-M. Weideman. Antenna position estimation through sub-sampled exponential analysis of signals in the near-field. URSI Radio Science Letters, 3, 2021.

[5] R. Louw, R.-M. Weideman, D.I.L. de Villiers, A. Cuyt, and S. J. Wijnholds. Antenna position estimation results from in-situ measurement data. In 2023 International Conference on Electromagnetics in Advanced Applications (ICEAA), 2023.

[6] R. Sengupta, A. Cuyt, F. Knaepkens, D. S. Prinsloo, T. Schäfer, and A. Bart Smolders. A fast exponential analysis and variable projection based method for linear array synthesis. IEEE Antennas and Wireless Propagation Letters, 2025.

[7] R.-M. Weideman, A. Cuyt, and D.I.L. de Villiers. Characterising the electric field ripple in reflector antennas using sub-sampled exponential analysis. IEEE Transactions on Antennas and Propagation, 72(7):5511–5519, 2024.

[8] Y. Zhang, A. Cuyt, W.-s. Lee, G. Lo Bianco, G. Wu, Y. Chen, and D. D.-U. Li. Towards unsupervised fluorescence lifetime imaging using low dimensional variable pro- jection. Opt. Express, 24(23):26777–26791, 2016.

11.2 Exponential Analysis for Net Operational Balance Forecasting

Anthony O'Hare
University of Stirling, United Kingdom

The Basel III framework, particularly through its Liquidity Coverage Ratio (LCR) requirement, obliges banks to hold a minimum amount of high-quality liquid assets based on an estimate of how much is expected to be withdrawn or "run off" during a specified period of stress.

Forecasting this minimum level (net operational deposit balances) is critical for effective liquidity management and strategic financial planning. Traditional time series forecasting methods often rely on assumptions of linearity, stationarity, and the continuation of past patterns. While useful

for stable environments, they frequently fall short when dealing with the complex, multi-modal, and often non-linear dynamics of financial data such as net operational deposit balances.

Matrix Pencil and ESPRIT can directly uncover and quantify the fundamental, often complex and noisy, exponential dynamics that drive these critical financial time series. This leads to more robust forecasts and a deeper understanding of balance behaviour than what traditional, simpler methods typically offer.

11.3 A Fast Exponential Analysis and Variable Projection Based Method for Linear Antenna Array Synthesis

Ramonika Sengupta
Eindhoven University of Technology, The Netherlands

Modern wireless communication systems frequently employ antenna arrays because of their high gain and beamforming capabilities. With increasing complexity, sparse arrays that utilize fewer antenna elements are becoming increasingly popular. In this context, exponential analysis has been explored as a tool for synthesizing linear antenna arrays with reduced element counts. However, many of these synthesis methods overlook the scan performance of the resulting arrays. Achieving a wide scan range remains particularly challenging, especially since the synthesized arrays are typically aperiodic.

In this talk, we explore some possible solutions to improve the scan performance of aperiodic arrays, using exponential analysis and variable projection. Numerical experiments demonstrate that with the given techniques it is possible to reduce the elements in an array, while maintaining a wide scan range for the synthesized array, and with directivity that is comparable to an array with more elements.

11.4 A new black box GCD algorithm using sparse Hensel lifting

Garrett Paluck
Simon Fraser University, Canada

Let a and b be polynomials in $\mathbb{Z}[x_1, \ldots, x_n]$ that are given by black boxes for their evaluation. We present a new GCD algorithm for recovering the monic GCD $g = \gcd(a, b)$ in $\mathbb{Q}[x_1, \ldots, x_n]$ in the sparse representation. Our algorithm recovers g one variable at a time from bivariate images obtained using bivariate Hensel lifting. We have implemented our algorithm in Maple.

Our algorithm has three practical advantages over previous black box algorithms. First, it is a modular GCD algorithm; it recovers the rational coefficients in g using Chinese remaindering and rational number reconstruction. Second, it can easily omit computation of the content of g in a chosen variable x which means it's faster for applications which need only the primitive part of g in x. Third, it recovers the square-free factorization of g which means it's faster when the square-free factors of g are all smaller than g.

In the talk we'll present our new GCD algorithm and benchmarks comparing it with previous work; we compare CPU time and the number of black box probes of the algorithms.

SPECIAL SESSION 12

Symbolic-Numeric Computation

The integration of symbolic and numeric techniques has become increasingly important in various fields of computational science and engineering. Symbolic-numeric computation (SNC) combines the power of exact symbolic manipulation with the efficiency of numerical methods, addressing complex problems that require both precision and computational scalability. This session aims to highlight the latest developments and applications of SNC, including hybrid algorithms, efficient implementations, and interdisciplinary uses. Topics of interest include, but are not limited to:

- Hybrid symbolic-numeric algorithms for solving equations
- Exact and approximate solutions in algebraic geometry
- Symbolic differentiation and numerical integration
- Symbolic-numeric methods for large-scale linear and nonlinear systems
- Applications in data science, machine learning, and optimization
- Symbolic-numeric approaches to differential equations and systems
- Tools, software, and frameworks supporting SNC

This session welcomes contributions that integrate symbolic and numeric techniques, focus on innovative methods, theoretical advancements, and practical applications. By bringing together researchers from diverse fields, we aim to encourage discussions on the challenges and opportunities in hybrid computation. We invite both theoretical and applied work, including novel algorithmic developments, computational frameworks, and real-world problem-solving approaches that leverage the strengths of both symbolic and numeric computation.

Session organizers

- Tülay Ayyıldız (Gebze Technical University, Turkey)
- Fabrice Rouillier (INRIA Paris, France)
- Elias Tsigaridas (INRIA Paris, France)

12.1 Static bounds for straight-line programs

Joris van der Hoeven, Grégoire Lecerf and Arnaud Minondo[1]
CNRS, École polytechnique, Institut Polytechnique de Paris, France

How to automatically determine reliable error bounds for a numerical computation? One traditional approach is to systematically replace floating point approximations by intervals or balls that are guaranteed to contain the exact numbers one is interested in. However, operations on intervals or balls are more expensive than operations on floating point numbers, so this approach involves a non-trivial overhead.

We will present several approaches to remove this overhead, under the assumption that the function f that we wish to evaluate is given as a straight-line program (SLP). We will first study the case when the arguments of our function lie in fixed balls. For polynomial SLPs, we next consider the "global" case where this restriction on the arguments is removed. We will also investigate the computation of bounds for first and higher order derivatives of f.

12.2 Copositive geometry of Feynman integrals

Máté L. Telek
Max Planck Institute for Mathematics in the Sciences, Germany

Copositive polynomials —that is, polynomials that are nonnegative on the nonnegative real orthant— are well-studied objects in real algebraic geometry and optimization. We connect these to the geometry of Feynman integrals in physics. The integral is guaranteed to converge if its kinematic parameters lie in the interior of the copositive cone.

In this talk, we will discuss several computational methods for certifying whether a given polynomial lies in the copositive cone. In particular, we show that Pólya's method can always be effectively applied to polynomials arising from Feynman integrals. The talk is based on a recent work with Bernd Sturmfels.

12.3 Solving bihomogeneous polynomial systems with a zero-dimensional projection

Matías Bender
Inria - École Polytechnique, France

In this talk, we study bihomogeneous systems defining, non-zero dimensional, biprojective varieties for which the projection onto the first group of variables results in a finite set of points. To compute (with) the 0-dimensional projection and the corresponding quotient ring, we introduce linear maps that greatly extend the classical multiplication maps for zero-dimensional systems, but are not those associated to the elimination ideal; we also call them multiplication maps. We construct them using linear algebra on the restriction of the ideal to a carefully chosen bidegree or, if available, from an arbitrary Gröbner bases. The multiplication maps allow us to compute

[1]Grégoire Lecerf and Arnaud Minondo have been supported by the French ANR-22-CE48-0016 NODE project. Joris van der Hoeven has been supported by an ERC-2023-ADG grant for the ODELIX project (number 101142171).

the elimination ideal of the projection, by generalizing FGLM algorithm to bihomogenous, non-zero dimensional, varieties. We also study their properties, like their minimal polynomials and the multiplicities of their eigenvalues, and show that we can use the eigenvalues to compute numerical approximations of the zero-dimensional projection. Finally, we establish a single exponential complexity bound for computing multiplication maps and Gröbner bases, that we express in terms of the bidegrees of the generators of the corresponding bihomogeneous ideal. This talk is based on joint work with Laurent Busé, Carles Checa and Elias Tsigaridas.

12.4 A symbolic-numeric method for certified eigenvalue localization

Baran Solmaz and Tülay Ayyıldız[2]
Gebze Technical University, Türkiye

Eigenvalues play a crucial role in nearly all areas of applied and theoretical science, with real eigenvalue locations offering critical insights for stability analysis, resonance phenomena, and physical system modeling. This work presents a hybrid approach for *certified real eigenvalue localization* for real matrices, within a computed spectrum. Our approach combines symbolic-numeric techniques: We integrate Hermite matrix certification with Gershgorin disk analysis and trace-based eigenvalue bounds. The method provides interval certifications while maintaining computational efficiency. Then we extend this approach for complex eigenvalues of complex matrices and obtain certified rectangular regions on the complex plane. We illustrate our approach on numerical examples

[2]Tülay Ayyıldız has been supported by the TÜBİTAK Project project number 122F138.

SPECIAL SESSION 13

Advances in Coding Theory: Algebraic, Combinatorial and Computational Methods

This special session will focus on the interplay between coding theory with special emphasis on algebraic, combinatorial, and computational methods. These include the exploration of algebraic and geometric methods for special classes of codes such as algebraic geometry codes, rank-metric codes, additive codes, and codes with automorphisms. Techniques from Delsarte and Levenshtein for code families and related combinatorial structures will also be explored. Additionally, the session will focus on computer algebra methods for determining the parameters of codes and related combinatorial structures.

Session organizers

- Peter Boyvalenkov (Bulgarian Academy of Sciences, Bulgaria)
- Cem Güneri (Sabanci University, Turkey)
- Ferruh Özbudak (Sabanci University, Turkey)

13.1 Characterization of Nearly Self-Orthogonal Quasi-Twisted Codes and Related Quantum Codes

Buket Özkaya
Middle East Technical University, Türkiye

Quasi-twisted codes are used here as the classical ingredients in the so-called Construction X for quantum error-control codes. The construction utilizes nearly self-orthogonal codes to design quantum stabilizer codes. We expand the choices of the inner product to also cover the symplectic and trace-symplectic inner products, in addition to the original Hermitian one. A refined lower bound on the minimum distance of the resulting quantum codes is established and illustrated. We report numerous record breaking quantum codes from our randomized search for inclusion in the updated online database.

13.2 On the complete characterization of a class of permutation trinomials in characteristic five

Burcu Gülmez Temür
Atılım University, Turkey

Let $\mathbb{F}_q$ be a finite field with q elements, where q is a prime power. A polynomial $g(x) \in \mathbb{F}_q[x]$ is called a permutation polynomial (PP) over $\mathbb{F}_q$ if $g(x)$ is a bijection of $\mathbb{F}_q$.

Due to their simple algebraic structure and extraordinary properties, there has been a great interest in permutation polynomials with a few terms, such as binomials or trinomials. Permutation polynomials are also very important in terms of their applications in areas such as cryptography, coding theory and combinatorial designs. As far as we know, the studies on permutation polynomials go back to the work done by Dickson and Hermite (see, [2] and [4]). In this paper, we address an open problem posed by Bai and Xia in [1]. We study polynomials of the form $f(x) = x^{4q+1} + \lambda_1 x^{5q} + \lambda_2 x^{q+4}$ over the finite field $\mathbb{F}_{5^k}$, which are not quasi-multiplicative equivalent to any of the known permutation polynomials in the literature. We find necessary and sufficient conditions on $\lambda_1, \lambda_2 \in \mathbb{F}_{5^k}$ so that $f(x)$ is a permutation monomial, binomial, or trinomial of $\mathbb{F}_{5^{2k}}$. This is a collaborated work done by Markus Grassl, Ferruh Özbudak, Buket Özkaya and B.G.T.

References

[1] Bai T., Xia Y., A new class of permutation trinomials constructed from Niho exponents, Cryptogr. Commun. 10, 1023–1036 (2018).
[2] Dickson, L.E., The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group, Ann. Math. 11, 65–120 (1896).
[3] Grassl, M., Özbudak, F., Özkaya, B., Gülmez Temür, B., Complete characterization of a class of permutation trinomials in characteristic five. Cryptogr. Commun. 16, 825–841 (2024).
[4] Hermite, Ch., Sur les fonctions de sept lettres, C.R. Acad. Sci. Paris 57, 750–757 (1863).

13.3 Some constructions of asymptotically optimal cyclic subspace codes

Chiara Castello and Paolo Santonastaso

University of Campania "L. Vanvitelli", Italy

A constant dimension subspace code $\mathcal{C}$ is a subset of the Grassmaniann $\mathcal{G}_q(n,k)$ endowed with the subspace distance. A cyclic subspace code $\mathcal{C}$ in $\mathcal{G}_q(n,k)$ is union of orbits of subspaces of $\mathbb{F}_{q^n}$ under the action of the multiplicative group of $\mathbb{F}_{q^n}$. In this talk, we introduce a new technique for constructing cyclic subspace codes with large cardinality and prescribed minimum distance. Using this new method, we provide new constructions of cyclic subspace codes in the Grassmannian $\mathcal{G}_q(n,k)$, where $k \mid n$ and n/k is a composite number, with minimum distance $2k-2$ and large size. Precisely, we prove that the resulting codes have sizes larger than those obtained from previously known constructions with the same parameters. Furthermore, we prove that our constructions of cyclic subspace codes asymptotically reach the Johnson bound for infinite values of n/k.

13.4 Scattered trinomials of $\mathbb{F}_{q^6}[X]$ in even characteristic

Giovanni Longobardi
University of Naples Federico II, Italy

(joint work with D. Bartoli, G. Marino and M. Timpanella)

In the last decades, Algebraic Geometry over finite fields has emerged as a powerful tool for investigating various objects closely associated with Galois Geometry, Coding Theory and Cryptography. In this talk, we will show an example of this approach through the study of a family of scattered polynomials defined over a finite field of even characteristic. Although several families of scattered polynomials have been investigated in recent years, most of them only exist in odd characteristics. In particular, in [1] and [2] the authors proved that the trinomial

$$f_c(X) = X^q + X^{q^3} + cX^{q^5}$$

of $\mathbb{F}_{q^6}[X]$ is scattered under the assumptions that q is odd and $c^2 + c = 1$. However, they explicitly noted that this is not the case when q is even.

Using tools of Algebraic Geometry in positive characteristic, we explore a different set of conditions on c under which this trinomial is scattered in the case of even q and we show that when q is sufficiently large, there are roughly q^3 elements $c \in \mathbb{F}_{q^6}$ such that $f_c(X)$ is scattered.

References

[1] B. Csajbók, G. Marino, F. Zullo. New maximum scattered linear sets of the projective line, *Finite Fields Appl.*, **54**:133-150, 2018.

[2] G. Marino, M. Montanucci, F. Zullo. MRD-codes arising from the trinomial $x^q + x^{q^3} + cx^{q^5} \in \mathbb{F}_{q^6}[x]$, *Linear Algebra Appl.* **591**:99-114, 2020.

13.5 Graph isomorphism and isomorphism of binary matrices

Iliya Bouyukliev and Maria Pashinska-Gadzheva[1]
Bulgarian Academy of Sciences, Bulgaria

This work explores an adaptation of the Weisfeiler-Leman (WL) algorithm, originally developed for graph isomorphism testing, to the domain of binary matrices.

[1]This research is supported by Bulgarian Science Fund under Contract KP-06-H62/2/13.12.2022

13.6 Enumeration of optimal binary and ternary linear codes with different hull dimensions

Stefka Bouyuklieva and Mariya Dzhumalieva-Stoeva[2]
St. Cyril and St. Methodius University of Veliko Tarnovo, Bulgaria

We present results related to the classification of binary and ternary linear codes, in which the codes are divided into different groups depending on the dimensions of their hulls. We pay special attention to some regularities that are noticeable when analyzing the obtained results.

13.7 On a spherical code with 2025 points

Peter Boyvalenkov
Bulgarian Academy of Sciences, Bulgaria

Joint work with Danila Cherkashin and Peter Dragnev

We consider a remarkable spherical code on $\mathbb{S}^{21}$ of cardinality 2025. Forbidding suitable distances to appear we define a class of so-called T-avoiding codes, where the set T correponds to the forbidden distances. We prove that this code is maximal when $T = (-4/11, -1/44)$, it is a minimal spherical 4-design when T is either $(-4/11, -1/44)$ or $(-1/44, 7/22)$, and, finally, it is universally optimal in the sense of Cohn-Kumar when T is again either $(-4/11, -1/44)$ or $(-1/44, 7/22)$.

13.8 Universal polarization of sharp codes in the Leech lattice

Peter Dragnev[3]
Purdue University Fort Wayne, USA

Given a spherical code $C \subset \mathbb{S}^{n-1}$ and a potential h, the discrete h-potential of C is given as $U_h(x, C) = \sum_{y \in C} h(x \cdot y)$. A spherical $\tau = 2k - 1$ or $\tau_{1/2}$-design (a τ-design with vanishing moments of order $\tau + 2$ and $\tau + 3$), that can be embedded in k or $k+1$ parallel hyperplanes is called *PULB*-optimal, i.e. attains a polarization universal lower bound below. For a PULB-optimal code C and very broad class of potentials the location of the global minima of $U_h(x, C)$ are universal and independent of h. Two PULB-optimal codes C and D are called PULB-optimal pair (C, D) if the universal minima of $U_h(x, C)$ are the points of D and vice versa, the universal minima of $U_h(x, D)$ are the points of C. We call a PULB-optimal pair maximal if D is the set of all universal minimal of $U_h(x, C)$ and vice versa. We shall show that some remarkable universally optimal codes embedded in the Leech lattice give rise to maximal PULB-pairs.

13.9 On the hulls of linear codes

Stefka Bouyuklieva[4]
St. Cyril and St. Methodius University of Veliko Tarnovo, Bulgaria

[2]This research is supported by Bulgarian Science Fund under Contracts KP-06-H62/2/13.12.2022 and FSD-31-328-09/23.04.2025

[3]Joint work with S. Borodachov, P. Boyvalenkov, D. Hardin, E. Saff, M. Stoyanova

[4]This research is supported by Bulgarian Science Fund under Contract KP-06-H62/2/13.12.2022

Some important properties of the hulls of linear codes over different finite fields will be presented. The numbers of codes of a given length and dimension but different hull dimensions will be compared. The idea of relative hulls will be discussed.

13.10 Resolutions of cyclic 2-(40,4,1) designs

Svetlana Topalova and Stela Zhelezova[5]
Bulgarian Academy of Sciences, Bulgaria

Let V be a finite set of v *points*, and $\mathcal{B} = \{B_j\}_{j=1}^{b}$ a finite family of k-element subsets of V, called *blocks*. A pair $(V, \mathcal{B})$ is a *Steiner system* S$(2, k, v)$ (a 2-$(v, k, 1)$ design) if any 2-element subset of V is contained in exactly one block of $\mathcal{B}$. There are $|\mathcal{B}| = b = v(v-1)/k(k-1)$ blocks in an S$(2, k, v)$ and each point is in $r = (v-1)/(k-1)$ blocks.

Let $(V, \mathcal{B})$ and $(V', \mathcal{B}')$ be two Steiner systems S$(2, k, v)$. They are isomorphic if there is a permutation of the points $\phi : V \to V'$ which maps each block $B \in \mathcal{B}$ to a block $B' \in \mathcal{B}'$, $\phi(B) = B'$. An authomorphism of an S$(2, k, v)$ is an isomorphism to itself. A Steiner system S$(2, k, v)$ is cyclic if it has an authomorphism of order v permuting its points in one cycle.

The necessary condition for the existence of an S$(2, 4, v)$ is $v \equiv 1, 4 (\mathrm{mod}\ 12)$ and it is sufficient [4]. A cyclic S$(2, 4, v)$ exists for all possible v except for $v = 16, 25, 28$ [8].

A parallel class R_i, $i = \{1, \ldots, r\}$ in an S$(2, k, v)$ is a set of v/k blocks which partition the point set. An S$(2, k, v)$ is resolvable if the collection of its blocks can be partitioned to r parallel classes. Such a partition is called a resolution. Two resolutions are isomorphic if at least one automorphism of the underlying Steiner system maps each block of the first resolution to a block of the second one. An automorphism of a resolution is an isomorphism to itself. A resolvable Steiner system S$(2, 4, v)$ exists iff $v \equiv 4 (\mathrm{mod}\ 12)$ [5].

The most studied Steiner systems are the S$(2, 3, v)$s known as Steiner triple systems (STS(v)s). A considerable amount of research has been done on S$(2, 4, v)$s too. Their resolvability is in the focus of the present paper.

A cyclic Steiner system can be cyclically resolvable if at least one of its resolutions has an automorphism permuting the points in one cycle. Such a resolution is called point-cyclic and can exists for $v \equiv k (\mathrm{mod}\ k(k-1))$. The smallest set of parameters which fulfills the necessary conditions for the existence of cyclically resolvable S$(2, 4, v)$s is S$(2, 4, 40)$.

There is a construction of cyclically resolvable S$(2, k, v)$s for $v = ku$, u - a prime number [3]. The considered parameters do not match this construction. There are no cyclically resolvable Steiner systems among the cyclic S$(2, 4, 40)$s. Resolutions of S$(2, k, v)$s are of interest in connection with binary LDPC codes [6]. In that case cyclic Steiner systems are preferable because they might allow faster decoding. Thus when the point-cyclic resolutions are missing, the other resolutions of the cyclic S$(2, 4, v)$s are of particular interest.

There are 10 cyclic S$(2, 4, 40)$s. One of them is the point-line design of $PG(3, 3)$ with an automorphism group of order $12\,130\,560$. All its $73\,343$ resolutions have been recently constructed by Betten [1]. The other nine cyclic S$(2, 4, 40)$s are with automorphism groups of orders 40, 80, and 160. We establish that three of them have altogether 1160 resolutions. We also investigate their automorphism groups and orbit structures.

[5]This research is partially supported by the Bulgarian National Science Fund under Contract No KP-06-H62/2/13.12.2022.

Nowadays the role of computers in algebraic combinatorics is important. Computer algebra systems are used to generate new interesting combinatorial objects and to find some of their useful properties. GAP (Groups, Algorithms, Programs) [2] is a system designed to consider different problems in discrete mathematics. Information about some of the known examples of S$(2, 4, v)$s can be found in [7], where they are given in the format of the GAP Design package. We use the group theory functionality of GAP and our own C++ implementations of different algorithms for the construction of resolutions. This way we obtain all resolutions of the cyclic S$(2, 4, 40)$s.

References

[1] Betten, A. The packings of PG(3,3). *Des. Codes Cryptogr.* 79: 583–595, 2016.

[2] GAP - Groups, Algorithms, Programming - a System for Computational Discrete Algebra, `http://www.gap-system.org/`. Last accessed: May 2025.

[3] Genma, M., Mishima, M., Jimbo, M. Cyclic resolvability of cyclic Steiner 2-designs. *J. Combin. Des.* 5(3): 177–187, 1997.

[4] Hanani, H. The existence and construction of balanced incomplete block designs. *Ann. Math. Stat.* 32: 361–386, 1961.

[5] Hanani, H., Ray-Chaudhuri, D.K., Wilson, R.M. On resolvable designs. *Discrete Math.* 3: 343–357, 1972.

[6] Johnson, S. J., Weller, S. R. Resolvable 2-designs for regular low-density parity-check codes. *IEEE T Commun.* 51(9): 1413–1419, 2003.

[7] Krcadinac, V. Steiner 2-designs, `https://web.math.pmf.unizg.hr/~krcko/results/steiner.html`. Last accessed: May 2025.

[8] Zhang, M., Feng, T., Wang, X. The existence of cyclic $(v, 4, 1)$-designs. *Des. Codes Cryptogr.* 90: 1611–1628, 2022.

13.11 Girth Analysis of Quantum Quasi-Cyclic LDPC Codes

Daniel Panario
Carleton University, Canada

Quantum error-correcting codes (QECCs) are vital for safeguarding quantum information from the detrimental effects of decoherence and quantum noise. This makes them crucial in quantum computing and communication. While quantum computers have the potential to solve problems much faster than their classical counterparts [4], they are highly susceptible to errors. Addressing these errors is a major challenge, and QECCs have become a key strategy to protect quantum information. The concept of QECCs was initially introduced in foundational works by Calderbank, Shor, and Steane [2] and [5]. The Calderbank-Shor-Steane (CSS) framework has provided a cornerstone for much of the subsequent research in the field.

Quantum quasi-cyclic LDPC (QQC LDPC) codes, like CSS codes have good structure and popular channel coding schemes. We investigate the use of fully connected quasi-cyclic LDPC (QC-LDPC) codes to build QQC-LDPC codes. It is known (experimentally) that the girth, that is, the length of the shortest cycles of the bipartite graph of its parity-check matrix, influences the code performance.

We prove [1] that QC-LDPC codes with column weight $\mathcal{J}$ at least 3, used to construct QQC-LDPC codes have girth at most 6. We present an efficient and practical method to obtain QQC-LDPC codes from QC-LDPC codes with $g = 8$ and $\mathcal{J} = 2$. Then, we extend our method to construct codes with $\mathcal{J} = 2$ and $g = 12$, thus reaching the largest possible girth [3].

References

[1] F. Amirzade, D. Panario and M.-R Sadeghi, "Girth Analysis of Quantum Quasi-Cyclic LDPC Codes", *Problems of Information Transmission* 60, 71–89, 2024.
[2] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Phys. Rev. A* 54, 1098–1105, 1996.
[3] M. P. C. Fossorier, "Quasi-cyclic low-density parity-check codes from circulant permutation matrices," *IEEE Trans. Inf. Theory* 50, 1788–1793, 2004.
[4] P. W. Shor, "Scheme for reducing decoherence in quantum memory", *Phys. Rev. A* 52, 2493–2496, 1995.
[5] A. M Steane, "Simple quantum error-correcting codes," *Phys. Rev. A* 54, 4741–4751, 1996.

13.12 On the minimum distance and covering radius of irredundant orthogonal arrays

Maryam Bajalan
Bulgarian Academy of Sciences, Bulgaria

Joint work with Peter Boyvalenkov

An orthogonal array (OA), denoted by $\mathrm{OA}(M, n, q, t)$, is an $M \times n$ matrix over an alphabet of size q such that every selection of t columns contains each possible t-tuple exactly M/q^t times. An irredundant orthogonal array (IrOA) is an OA with the additional property that, in any selection of $n - t$ columns, all resulting rows are distinct. IrOAs were first introduced by Goyeneche and Życzkowski in 2014 to construct t-uniform quantum states without redundant information. Beyond their quantum applications, we focus on IrOAs as a combinatorial problem. Using a characterization of IrOAs via their minimum distance we prove that for any linear code, either the code itself or its Euclidean dual forms a linear IrOA. In the special case of self-dual codes, both the code and its dual yield IrOAs. Moreover, we construct new families of linear IrOAs based on self-dual, Maximum Distance Separable (MDS), and MDS-self-dual codes. Finally, we establish bounds on the minimum distance and covering radius of IrOAs.

SPECIAL SESSION 14

Finite Fields and Applications

This session's focus is on the rich and diverse world of finite fields which play a crucial role in various branches of mathematics like algebra, number theory, combinatorics, finite geometry and more.

Finite fields also provide the foundation for many aspects of secure and robust communications in applied areas such as coding theory, cryptography, and information theory.

We aim to bring together a group of researchers to discuss and showcase the latest advancements in the theory, applications and implementations of finite fields.

Session organizers

- Daniel Panario (Carleton University, Canada)
- Theodoulos Garefalakis (University of Crete, Greece)

14.1 A new tool for differential analysis of functions in characteristic 2

Alev Topuzoğlu
Sabancı University, Turkey

Recent advances in differential cryptanalysis necessitate acquiring increasingly more knowledge of differential properties of S-boxes. Here we present a new tool enabling a detailed differential analysis of functions $G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$.

Given a function $G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, the behavior of D_aG, the *first derivative of G in the direction* $a \in \mathbb{F}_{2^n}^* = \mathbb{F}_{2^n} \setminus \{0\}$, where $D_aG(x) = G(x) + G(x+a)$, plays a major role in assessing the resistance of G against the differential attack and its refinements.

A natural way of studying the differential properties of G, as is recently exhibited in [1], is to consider the so-called *difference square* corresponding to G, which is defined as follows. By fixing an ordering of the elements of $\mathbb{F}_{2^n}$, therefore putting $\mathbb{F}_{2^n} = \{x_1 = 0, x_2 = 1, \ldots, x_{2^n}\}$, it is the $2^n - 1$ by 2^n array, where the a-th row $\Delta_a(G)$, $a \in \{x_2, \ldots, x_{2^n}\}$, consists of the derivatives $D_aG(x_1), \ldots, D_aG(x_{2^n})$. This view point leads to some unexpected new results, for instance, finding the partial quadruple system associated to G, or the number of vanishing flats with respect to G for some particular G.

It is shown in [1] that some interesting patterns in difference squares emerge, which motivate the introduction of a new concept, the *APN-defect* of G, which can be thought of as measuring the distance of G to the set of almost perfect nonlinear (APN) functions.

The aim of this talk is to explain how this measure can be used to identify *quasi-APN* functions, which behave favorably in terms of their differential properties, how to calculate it for some functions of interest, and why a careful study of difference squares may lead to the construction of new APN functions.

This is joint work with Nurdagül Anbar and Tekgül Kalaycı.

References

[1] Nurdagül Anbar, Tekgül Kalaycı, Alev Topuzoğlu. Analysis of functions of low differential uniformity in characteristic 2: A new approach (I). *Submitted*, 2024.

14.2 Algebraic and SAT Methods for Classes of Covering Arrays

Dimitris E. Simos
Salzburg University of Applied Sciences, Austria

In this work, we survey the current state-of-the-art for the generation of classes of covering arrays, such as optimal and sequence covering arrays, using methods originating from computer algebra as well as their hybridization with SAT solvers. Covering arrays are discrete structures where all t-way interactions of input parameters are covered up to a strength t and they are used in various fields of computer science, software engineering and cyber security among others. Sequence covering arrays consist of sequences, such that all subsequences with pairwise different entries of some length are covered, sharing similar properties like covering arrays, where they originate from the necessity of defining a rigorous mathematical structure in event-based testing. Concrete instances of covering arrays for given parameters will arise as points in a generated variety of a system of multivariate polynomial equations with Groebner Bases playing an important

role [1]. In addition, for sequence covering arrays, we will provide various algebraic models taking the form of multivariate polynomial systems of equations and are then processed via supercomputing by a Groebner Basis solver in order to compute solutions from them [2]. For the cases where theoretical constructions on a tuple-modelling level are not possible, we will employ various SAT encodings in conjunction with greedy techniques (e.g. IPO-strategy [3]). We conclude with the current open problems for generation of (sequence) covering arrays which lie in the intersection of discrete mathematics, computer algebra and applied computer science.

References

[1] B. Garn and D.E. Simos. Algebraic Modelling of Covering Arrays. *ACA '15: Applications of Computer Algebra, Springer Proceedings in Mathematics and Statistics*, pp.149–170, 2017.

[2] M. Koelbing, B. Garn, E. Iurlano, I.S. Kotsireas and D.E. Simos. Algebraic and SAT models for SCA generation. *Applicable Algebra in Engineering, Communication and Computing*, 36:173–222, 2025.

[3] I. Hiess, L .Kampel, M. Wagner and D.E. Simos. IPO-MAXSAT: The In-Parameter-Order Strategy combined with MaxSAT solving for Covering Array Generation. *SYNASC '22: Proceedings of the 24th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing*, pp. 71–79, 2022.

14.3 Automatic Sequences Along Polynomial Subsequences and Their Applications

Ísabel Pirsic and Domingo Gómez-Pérez
Universidad de Cantabria, Spain

Pseudorandom sequences are crucial in various fields, particularly in cryptography. These sequences, which must exhibit high entropy and efficient implementation, are essential for generating nonces, session keys, and parameters in cryptographic systems, among other uses. Due to their deterministic nature, pseudorandom sequences can be analyzed to identify regularities and understand potential weaknesses in the form of patterns.

Automatic sequences are families of sequences generated by formal automata. This category includes, but is not limited to, Thue-Morse, Rudin-Shapiro and paper folding sequences. In this talk, we introduce a new general family, the CAP sequences, which encompasses many previously studied sequences. We then explore the problem of studying polynomial subsequences of these sequences, specifically when they become constant. Additionally, we consider the converse problem: given a polynomial, determine a nontrivial CAP sequence which becomes constant on that polynomial.

Thus we exhibit the necessity to understand well the automatic sequence family to which the polynomial subsequence paradigm is applied for cryptographic purposes.

We conclude the presentation with a software implementation and some open problems.

14.4 Further results on covering radii of some codes and their connections

Ferruh Özbudak
Sabancı University, Turkiye

The covering radius is a basic geometric parameter of a code. It has various applications, including decoding, data compression, testing, write-once memories, and combinatorics in general. There are important connections to arithmetic and geometry over finite fields. In this paper, we survey some of the recent results, provide some new results and explain some aspects of the connections to the arithmetic and geometry over finite fields.

The research of Ferruh Özbudak is supported by TÜBİTAK under Grant 223N065

14.5 Normal and primitive normal elements with prescribed traces in intermediate extensions of finite fields

Giorgos Kapetanakis
University of Thessaly, Greece

In this talk, I will first present a joint work with A.C. Mazumder and D.K. Basnet, where we study the existence and distribution of elements in finite field extensions with prescribed traces in several intermediate extensions that are also either normal or primitive normal. In the former case, we fully characterize the conditions under which such elements exist and provide an explicit enumeration of these elements and, in the latter case, we provide asymptotic results.

Then, I will briefly discuss possible applications of these techniques and results to other finite field problems.

14.6 Quadratic-like permutations over $\mathbb{F}_2^n$

Irene Villa
University of Trento, Italy

Among the so-called (Boolean) (n, m)-functions, $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, those that are balanced present a particular interest in discrete mathematics. Among balanced functions, those such that $m = n$, that is, (n, n)-permutations, are of a still more specific interest.

In this work, we study the class of permutations whose component functions all admit a derivative equal to constant function 1 (this property itself implies balancedness). We call these functions *quadratic-like permutations*, since all permutation of degree 2 have this property. We study this class of functions, showing that we can have quadratic-like permutations of degree greater than 2 and we can have permutations not quadratic-like. We analyse how the property behaves under some equivalence transformations, and we study the "reversed" property: every derivative in a nonzero direction has a component function equal to constant function 1. We study some known classes of permutations, such as Feistel permutations, crooked permutations and power permutations, and we show that many of them satisfy this property (and also the "reversed" one). We provide also some primary and secondary constructions of quadratic-like permutations.

This is a joint work with Claude Carlet.

14.7 Invariant Polynomials and Cyclic Line Spreads

John Sheekey
University College Dublin, Ireland

Flag-transitive linear spaces have been fully classified for all but a small class of possible automorphism groups. For one of the remaining open cases, which arise from line-spreads fixed by a cyclic group, Bamberg and Pauley showed an equivalent characterisation in terms of polynomials $P(x) \in \mathbb{F}_{q^2}$ over a finite field with certain properties. The requirements on $P(x)$ are very similar, though not identical, to requirements for a related polynomial to define a permutation.

In [1] we fully solved the case of cubic polynomials using this approach. Key to the method involved the factorisation of a related two-variable polynomial $H_P(z, w)$, or plane curve. In this work we study the case of polynomials of arbitrary degree which define a flag-transitive linear space. We focus on the case where the aforementioned $H_P(z, w)$ splits into factors of low degree.

We show that this requires that $P(x)$ is invariant under certain elements $[\Psi]$ of $\mathrm{PGL}(2, \overline{\mathbb{F}_q})$. Polynomials of this form have been well-studied, from Stichtenoth-Topuzoglu, through Brochero Martinez-Garefalakis-Reis-Tzanaki, and beyond. In [2], [3] we prove further necessary conditions on $[\Psi]$ and $P(x)$, construct new families generalising those of Feng-Lu, and classify some small degrees. We will present some remaining open problems.

References

[1] Cian Jameson and John Sheekey. Cyclic 2-Spreads in $V(6, q)$ and Flag-Transitive Affine Linear Spaces, *Finite Fields and their Applications*, 98:102463, 2024.

[2] Cian Jameson. Classifying Flag-Transitive Linear Spaces using Cyclic Line-Spreads and Orbit Polynomials, *PhD Thesis*.

[3] Cian Jameson and John Sheekey. Orbit Polynomials and Cyclic Line Spreads, *in preparation*.

14.8 Nilpotent linearized polynomials and applications

Lucas Reis
Universidade Federal de Minas Gerais, Belo Horizonte, Brazil

We introduce and investigate nilpotent linearized polynomials (NLPs) over finite fields, examining their arithmetic properties as well as structural aspects derived from linear algebra. In particular, we present a method for constructing permutations of finite fields using NLPs and analyze the properties of these permutations, including cycle decomposition and the presence of fixed points. Special attention is given to the case of binary fields (fields of characteristic two), where we develop a systematic approach for generating NLPs (and thus permutations) by leveraging trace orthogonal bases.

14.9 New covering arrays of strength-4 and q symbols from three truncated Möbius planes in $PG(3, q)$, for odd prime power q

Lucia Moura
University of Ottawa, Canada

A strength-t covering array of size N, denoted by $\mathrm{CA}(N; t, k, v)$, is an $N \times k$ array over a v-set of symbols such that for any t-set of columns, each t-tuple occurs at least once in a row. Raaphorst et al. [3] construct a $\mathrm{CA}(2q^3 - 1; 3, q^2 + q + 1, q)$ from two projective planes, $\mathrm{PG}(2, q)$, on the same set of points such that any line in one plane intersects any line in the other plane in at most 2 points. In [2], Colbourn et al. call two such projective planes "orthogoval"; they study sets of

mutually orthogoval projective and affine planes, and discuss their connections to covering arrays. The covering arrays in [3] still hold the record of best size for these parameters for any prime power $q \geq 4$ [1].

Our present work extends the result by Raaphorst et al. to construct arrays of strength 4. A k-cap in a projective geometry is a set of k points no three of which are collinear. In $\mathrm{PG}(3, q)$, an ovoid is a maximum-sized k-cap with $k = q^2+1$. Its plane sections (circles) form a 3-$(q^2+1, q+1, 1)$ design, called a Möbius plane of order q. For q an odd prime power, we prove the existence of three truncated Möbius planes, such that for any choice of circles from each plane, their intersection size is at most three. From this, we construct a strength-4 covering array $\mathrm{CA}(3q^4 - 2; 4, \frac{q^2+1}{2}, q)$, for every odd prime power q. For $q \geq 11$, these covering arrays improve the size of the best-known covering arrays with the same parameters by $\sim 25\%$ [1]. These arrays can be easily constructed using linear-feedback shift-register sequences over finite fields. This is joint work with Kianoosh Shokri and Brett Stevens.

References

[1] C. J. Colbourn, Covering Array Tables, available at:
`https://github.com/ugroempi/CAs/blob/main/ColbournTables.md`, November 2024.

[2] C. J. Colbourn, C. Ingalls, J. Jedwab, M. Saaltink, K. W. Smith, and B. Stevens, Sets of mutually orthogoval projective and affine planes, *Combinatorial Theory* **1** (2024),#8.

[3] S. Raaphorst, L. Moura and B. Stevens, A construction for strength-3 covering arrays from linear feedback shift register sequences, *Designs, Codes and Cryptography* **76** (2014), 949–968.

14.10 Factoring Multilinear Boolean Polynomials

Michael Monagan
Simon Fraser University, Canada

We present two new algorithms for factoring multilinear boolean polynomials. The first is a Monte Carlo algorithm. The second is a deterministic algorithm based on recursive GCD computations. We've implemented both algorithms in C and also Emelyanov and Ponomaryov's FDE algorithm for comparison. Our Monte Carlo algorithm is much faster than their FED algorithm and our GCD algorithm is much faster than our Monte Carlo algorithm. But we do not know the complexity of our GCD algorithm.

14.11 On constructing bent functions from cyclotomic mappings

Qiang Wang
Carleton University, Canada

A Boolean function f in n variables with $f(0) = 0$ is bent if and only if the Cayley graph defined on $\mathbb{Z}_2^n$ by the support of a Boolean function is a strongly regular with parameters $(2^{2n}, 2^{2n-1} + \varepsilon 2^{n-1}, 2^{2n-2} + \varepsilon 2^{n-1}, 2^{2n-2} + \varepsilon 2^{n-1})$, $\varepsilon = \pm 1$. These bent functions are known as maximally nonlinear, which are as different as possible from the set of all linear and affine functions when measured by Hamming distance between truth tables. In this talk, we discuss some generic construction of Boolean bent functions from cyclotomic mappings. In particular, three generic constructions from this new perspective are obtained by considering Dillon functions, Niho functions and Kasami functions as different branch functions respectively. As a result, several infinite classes

of bent functions belonging to the $\mathcal{PS}_{ap}$ class, class $\mathcal{H}$ and the completed $\mathcal{MM}$ class are derived, thereby providing simple representations of known classes of bent functions through cyclotomic mappings. Moreover, computer experiments show that examples of bent functions outside these three well-known classes can also be obtained by selecting other branch functions.

14.12 Bent partitions, vectorial dual-bent functions, and association schemes

Tekgül Kalaycı
University of Klagenfurt, Austria

The recently introduced generalized semifield spreads are bent partitions of $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$, which are constructed from presemifields with a certain property, called right $\mathbb{F}_{p^k}$-linearity. Bent partitions have similar properties as spreads. In particular they yield a large number of bent functions and amorphic association schemes. We show that with right $\mathbb{F}_{p^k}$-linear presemifields, one can obtain a large variety of vectorial dual-bent functions, which yield association schemes that are not necessarily amorphic. More generally, we show that for $1 < s \leq m$, vectorial dual-bent functions from $\mathbb{V}_{2m}^{(p)}$ to $\mathbb{V}_{s}^{(p)}$, whose components are either all regular or all weakly regular but not regular, give rise to p^s-class association schemes on $\mathbb{V}_{2m}^{(p)}$.

SPECIAL SESSION 15

Reliable numerical computing and differential equations

One of the key advantages of computer algebra and symbolic computation is the mathematical exactness of all computed results. This session concerns a similar goal of exact mathematical computations for objects of a more analytic nature, through numerical approximations with provable error bounds. One particularly important application concerns the reliable integration of differential equations and the reliable evaluation of special functions. More generally, topics of interest include, but are not limited to:

- Logical foundations of reliable computation.
- Interval and ball arithmetic.
- High performance implementations of reliable algorithms.
- Reliable evaluation of special functions.
- Reliable integration of dynamical systems.
- Reliable homotopy continuation.
- Effective computations with analytic functions.
- Other applications of reliable computation.
- Mathematical software for reliable computations.

We welcome both theoretical and practical contributions as well as applications. The scope is wide and intended to encourage discussions and new collaborations during the conference.

Session organizers

- Joris van der Hoeven (CNRS, École polytechnique, France)
- Grégoire Lecerf (CNRS, École polytechnique, France)

15.1 Proudfoot-Speyer degenerations of scattering equations

Barbara Betti, Viktoriia Borovik, Simon Telen
Max Planck Institute for Mathematics in the Sciences, Leipzig, Germany

We study scattering equations of hyperplane arrangements from the perspective of combinatorial commutative algebra and numerical algebraic geometry. We formulate the problem as linear equations on a reciprocal linear space and develop a degeneration-based homotopy algorithm for solving them. We apply our methods to CHY scattering equations and discuss applications with particle physics.

15.2 Vector-friendly numbers with n-word precision

Fredrik Johansson
Inria & IMB (UMR 5251), France

In many computer algebra applications, we need to reliably manipulate vectors or matrices of real or complex numbers with "medium" precision, e.g. in the range 20 to 1000 digits. We present an implementation of floating-point vectors optimized for this task in FLINT and discuss extensions to ball arithmetic.

15.3 Logical Completeness of Differential Equations

Long Qian
Carnegie Mellon University, USA

Differential equations are fundamental across many disciplines, frequently used in modelling systems with continuous dynamics. It is therefore important to be able to correctly prove properties of differential equations, especially in safety-critical situations. Concretely, let $x' = f(x)$ be a n-dimensional differential equation with $\phi(x, t) : \mathbb{R}^n \times \mathbb{R} \to \mathbb{R}^n$ denoting its flow (assuming global existence for brevity). For a set of initial values $I \subseteq \mathbb{R}^n$ and a time interval $[0, T]$, common properties of interest include:

- Safety: Let $S \subseteq \mathbb{R}^n$ be a set of safe values, is it true that for every $x_0 \in I$, the trajectory of x_0 following $x' = f(x)$ stays in S on the time interval $[0, T]$? I.e. is the following formula valid?

$$\forall x_0 \in I \, \forall t \in [0, T] \; \varphi(x_0, t) \in S$$

- Liveness: Let $G \subseteq \mathbb{R}^n$ be a set of goal values, is it true that for every $x_0 \in I$, the trajectory of x_0 following $x' = f(x)$ reaches G on the time interval $[0, T]$? I.e. is the following formula valid?

$$\forall x_0 \in I \, \exists t \in [0, T] \; \varphi(x_0, t) \in G$$

One approach to validating such properties is to proceed quantitatively, computing numerical approximations to the reachable sets. However, the correctness of such methods are generally difficult to guarantee due to their numerical nature. Alternatively, one can also take a more qualitative approach, where a (small) set of general axioms concerning differential equations are proven to

be valid, and properties of ODEs are established deductively by iteratively applying such axioms. Consequently, the correctness of such proofs only depend on the validity of a small set of core axioms, and can be independently verified by theorem provers implementing this logical framework [1]. This logical system is called *differential dynamic logic* [2].

However, as such qualitative axioms are symbolic and qualitative, they are seemingly less capable than quantitative approaches at validating inherently numerical properties of differential equations. Naturally, one can ask for which class of properties can such qualitative axioms validate? Equivalently, is differential dynamic logic *complete* for certain class of properties? In joint work with André Platzer [3], we show that completeness for safety and liveness properties hold when the sets in question I, S, G are all first-order definable, I is compact and S, G both open.

References

[1] Nathan Fulton, Stefan Mitsch, Jan-David Quesel, Marcus Völp, and André Platzer. 2015. KeYmaera X: An Axiomatic Tactical Theorem Prover for Hybrid Systems. In *Automated Deduction - CADE-25 - 25th International Conference on Automated Deduction, Berlin, Germany, August 1-7, 2015, Proceedings (LNCS, Vol. 9195)*, Amy P. Felty and Aart Middeldorp (Eds.). Springer, Berlin, Germany, 527–538. https://doi.org/10.1007/978-3-319-21401-6_36

[2] André Platzer. 2008. Differential Dynamic Logic for Hybrid Systems. *J. Autom. Reason.* 41, 2 (2008), 143–189. https://doi.org/10.1007/S10817-008-9103-8

[3] André Platzer and Long Qian. 2024. Axiomatization of Compact Initial Value Problems: Open Properties. arXiv:2410.13836 [cs.LO] https://arxiv.org/abs/2410.13836

15.4 Braid monodromy computations using certified path tracking

Alexandre Guillemot, Pierre Lairez
Inria Saclay, France

Let $f \in \mathbb{C}[t, x]$. The set of roots of f in x when t moves continuously along a loop in $\mathbb{C}$ defines a braid, provided that t avoids a certain set of critical values. Artin proved that braids can be described in terms of elementary generators, and our goal is to compute such a decomposition for the braid induced by the displacement of the roots of f. Starting with the algebraic input f, we first numerically track its roots using certified homotopy continuation. This procedure outputs disjoint tubular neighborhoods each containing a strand of the induced braid. Although this output is by nature numerical, we can recover the braid expressed in terms of Artin's generators from it. This discrete description is certified, even though the intermediate step involves numerical computations. We provide a Rust implementation of the second step that can be piped with Algpath, a certified path tracking software, allowing for certified braid monodromy computations.

15.5 Some challenges and applications for continuation methods for solving algebraic systems

Fabrice Rouillier
Inria Paris, France

In this contribution, we describe some recent applications where we have combined symbolic and numerical methods for applications in robotics and control theory. The main focus is on solving algebraic systems while guaranteeing the result, i.e., the real nature of the solutions and their uniqueness in a region, or on certifying real-time methods with strict constraints on their implementation, or on certifying robot movements in a given workspace. We have deployed basic continuation methods (Newton+Kantorovitch for certification) and we hope, through this talk, to motivate the community to propose more efficient or easier-to-use methods.

SPECIAL SESSION 16

Solving Matrix and Tensor Equations

The researches on the solvability conditions and the structural representations of solutions to matrix and tensor equations have been one of the important topics in algebra for a long time. Nowadays as one important part of contemporary mathematics, matrix and tensor equations are widely and heavily used in many areas such as computer vision, data mining, system and control theory, and information science. No matter concerning the development of matrix and tensor theory or solving practical problems, further studying on solutions for matrix and tensor equations is essential.

The topics in this special session mainly focus on the solvability conditions, general and numeric solutions, structural representations and extremal ranks of the solutions to some matrix and tensor algebraic equations and coupled generalized Sylvester matrix (tensor) equations over various algebraic structures including fields, quaternions and general rings. Moreover, we will explore efficient symbolic and numeric computing algorithms for finding solutions and their applications in image processing, system and control theory, etc.

This special session will be an important opportunity for experts in linear algebra, matrix and tensor theory, ring theory and computer science to exchange ideas, problems and work together.

Session organizers

- Dragana Cvetkovic Ilic (Department of Mathematics, University of Nis, Serbia)
- Qingwen Wang (Department of Mathematics, Shanghai University, Shanghai, China)
- Yang Zhang (Department of Mathematics, University of Manitoba, Winnipeg, Canada)

16.1 On minor prime factorization for rank-deficient multivariate polynomial matrices

Dingkang Wang
Academy of Mathematics and Systems Science, Chinese Academy of Sciences, China

Multivariate polynomial matrices are fundamental objects in symbolic computation and commutative algebra, and their associated factorization problems have long constituted important research topics in fields such as multidimensional systems and signal processing. Building on Youla and Gnavi's analysis of the structural theory for multidimensional systems in the 1970s, factorizations of multivariate polynomial matrices have become a key research direction for mathematicians and engineers. Minor prime factorization of multivariate polynomial matrices is a critical subproblem in this area, where factorization algorithms for bivariate polynomial matrices play an important role in mu-basis computation for rational parametric surfaces. We focus on minor prime factorization of rank-deficient multivariate polynomial matrices. We first establish an algebraic relationship between a rank-deficient polynomial matrix and its arbitrary row-full-rank submatrix. Subsequently, a necessary and sufficient condition for the existence of minor prime factorization in the rank-deficient case is rigorously derived. Finally, an algorithm is presented, accompanied by experimental results demonstrating its computational efficiency. This is a joint work with Dong Lu.

16.2 The generalized hand-eye calibration equation and its application

Qing-Wen Wang
Shanghai University, P. R. China

In the field of robotics research, a crucial applied problem is the hand-eye calibration issue, which involves solving the matrix equation $AX = YB$. However, this matrix equation is merely a specific case of the generalized Sylvester-type dual quaternion matrix equation $AX-YB = C$, which also holds significant applications in system and control theory. Therefore, we in this talk establish the solvability conditions of this generalized Sylvester-type dual quaternion matrix equation and provide a general expression for its solutions when it is solvable. As an example of applications, we design a scheme for color image encryption and decryption based on the generalized Sylvester-type dual quaternion matrix equation. From the experiment, it can be observed that the decrypted images are almost identical to the original images. Therefore, the encryption and decryption scheme designed using this dual quaternion matrix equation is highly feasible.

16.3 Fixed-Time Tensor Gradient Neural Network for Online Sylvester Tensor Equation Solving

Mengyan Xie
Shanghai Ocean University, P. R. China

This presentation introduces a fixed-time convergent Tensor Gradient-based Neural Network (TGNN) model for real-time resolution of the generalized Sylvester tensor equation:

$$\sum_{n=1}^{N} \mathcal{X}(t) \times_n A_n = \mathcal{B}$$

in real-time applications. The key innovation lies in a newly designed activation function that guarantees fixed-time convergence, rigorously proven through theoretical analysis. We systematically compare this activation function with four existing nonlinear alternatives under the TGNN framework, providing tight upper bounds for their convergence times. Numerical experiments on two benchmark problems demonstrate the superior convergence speed and computational robustness of our method.

16.4 The $\mathcal{A}_\alpha$-spectral radius of uniform hypergraphs

Xiao-Dong Zhang
Shanghai Jiao Tong University, P. R. China

For a k-uniform hypergraph G, let $\mathcal{D}(G)$ and $\mathcal{A}(G)$ be the diagonal tensor and the adjacency tensor of G, respectively.The $\mathcal{A}_\alpha$-spectral radius of G is defined as the spectral radius of the tensor $\mathcal{A}_\alpha(G) = \alpha\mathcal{D}(G) + (1-\alpha)\mathcal{A}(G)$, where $0 \leq \alpha < 1$. In this talk, we establish some sharp lower and upper bounds for the $\mathcal{A}_\alpha$-spectral radius of a connected k-uniform hypergraph. This work is joined with Peng-Li Zhang (Shanghai University of International Business and Economics).

16.5 Solving reduced biquaternion tensor equations and applications

Yang Zhang
University of Manitoba, Canada

We first develop an algorithm for computing the singular value decomposition (SVD) of a third-order reduced biquaternion tensor via a new Ht-product. As theoretical applications, we define the Moore-Penrose inverse of a third-order reduced biquaternion tensor and consider its characterizations via its SVD. Using Moore-Penrose inverses, we mainly discuss the general (or Hermitian) solutions to reduced biquaternion tensor equation $\mathcal{A} *_{Ht} \mathcal{X} = \mathcal{B}$ as well as its least-squares solutions. Finally, we develop two novel fast algorithms and apply them in color video compression and deblurring, both of which perform better than the compared algorithms, especially in CPU Time. This is a joint work with Cui-E Yu, Xin Liu, and Hui Luo.

SPECIAL SESSION 17

Combinatorial and Geometrical Methods in Contemporary Coding Theory

The theory of error-correcting codes has inspired many mathematicians who were interested in applying techniques from algebra and discrete mathematics in order to progress on questions in information processing. Coding theory lies at the intersection of several disciplines in pure and applied mathematics such as algebra, number theory, probability theory, statistics, combinatorics, complexity theory, and statistical physics, which all have helped in the past to increase our knowledge in communication theory. The design of error-correcting codes for the reliable transmission of information across noisy channels plays a crucial role in the modern era due to the massive overall communication traffic. To this aim, it has been necessary to develop sophisticated algebraic, combinatorial and geometric tools in order to construct codes that can correct as many errors as possible in a very efficient way.

This session is focused on the application of computer algebra to coding theory which, together with classical and new methods from combinatorics and geometry, can be used to obtain several and important results, such as construction of optimal codes, definition of efficient encoding and decoding algorithms and the study of algebraic, geometric and combinatorial problems arising from practical problems in coding theory. We wish to invite talks about recent results and developments in coding theory, including but not restricted to:

- Algebraic coding theory
- Rank/sum-rank metric codes
- Algebraic geometry codes
- Graph theory methods in coding theory
- Convolutional codes
- Quantum codes
- Algebraic decoding algorithms
- Combinatorial algorithms
- Computational results
- Related algebraic and combinatorial structures

Session organizers

- Gianira N. Alfarano (University of Rennes, France)
- Giovanni Longobardi (Università degli Studi di Napoli Federico II, Italy)

17.1 Hamming weight distributions of linear simplex codes over finite chain rings and their Gray map

Cristina Fernández-Córdoba, Sergi Sánchez-Aragón and Mercè Villanueva
Universitat Autònoma de Barcelona, Spain

A linear code of length n over a finite chain ring R with residue field $\mathbb{F}_q$ is a R-submodule of R^n. A R-linear code is a code over $\mathbb{F}_q$ (not necessarily linear) which is the generalized Gray map image of a linear code over R. In this work, we present the construction of linear simplex codes over R and their corresponding R-linear codes of type α and β. Moreover, we show the fundamental parameters of these codes as well as their complete weight distributions. We also study whether these simplex codes are optimal with respect to the Griesmer-type bound.

17.2 Construction of LDPC convolutional codes from Latin squares

Elisa Junghans
TU Ilmenau, Germany

Low-density parity-check (LDPC) codes are known for their capacity approaching performance with message passing algorithms as well as their low encoding and decoding complexity. These properties can be generalized for (time-varying) convolutional codes. For the decoding algorithms to perform well, it is desirable to maximize the girth of the associated Tanner graph. While it is possible to find well-performing LDPC codes via random search, it is still desirable to construct such codes that additionally allow for some kind of compact representation in order to store them efficiently.

We present a construction for periodically time-varying LDPC convolutional codes using a special class of orthogonal Latin squares. To achieve a girth up to 12, we apply several lifting steps to the original construction. This construction depends only on the Latin squares and well-determined lifting steps. This allows for a very compact representation of these codes.

17.3 Construction of partial unit-memory MDP convolutional codes with low encoding and decoding complexity

Julia Lieb
TU Ilmenau, Germany

Maximum Distance Profile (MDP) convolutional codes are error-correcting codes that can correct a maximum amount of errors for a specific delay constraint. To minimize encoding and decoding complexity when using MDP codes, researchers have been trying to construct these codes over possibly small finite fields, which turns out to be a difficult task. However, up to our knowledge, other aspects influencing complexity have not been investigated yet.

We present constructions for partial unit-memory MDP codes with reduced encoding and decoding complexity via structured and sparse generator matrices over small finite fields. In particular, we present a matrix completion framework that extends a structured MDS matrix over a small field to a sparse sliding generator matrix of an MDP code.

This is joint work with Sakshi Dang, Okko Makkonen, Pedro Soto and Alex Sprintson.

17.4 Equivalences of rank distance codes

Valentino Smaldore
Università degli Studi di Padova, Italy

This paper investigates the equivalence issue for rank distance codes in $\mathbb{F}_q^{n\times n}$ of dimension $2n$. The techniques used involve the analysis of the corresponding linearized polynomials. Indeed, under certain assumptions, the right idealizer of the code is isomorphic to the algebra of 2×2 matrices stabilizing the graph of the polynomial in the affine plane $AG(2, q^n)$.

17.5 On some properties of the Gray map

Anna-Lena Horlemann, Adrien Pasquereau and Carlos Vela Cabello
University of St. Gallen, Switzerland

We discuss the properties of the Gray map and its generalizations. Within our new framework, one can recover many well-known properties of the Gray map, but also identify some original behaviors. First, we show that the Gray map can be factored as a mapping to a multivariate polynomial ring followed by an evaluation over a projective point set. This provides an interpretation of the Gray map in terms of evaluation of functions. Under this association, it follows that the linearity defect of the image of the code, e.g., its rank and its kernel (in the nonlinear sense), can be characterized by the structure of this set of functions. In particular, we derive some local principles that allow to reduce the study of the image code to a shortened code over a logarithmically smaller support. In parallel, we pay a specific attention to the practical costs for manipulating these invariants: for example, we provide a very efficient algorithm to invert the Gray map.

17.6 Characteristic polynomial of linearized polynomials

Luca Bastioni
University of South Florida, USA

Let q be a prime power, and $\mathbb{F}_q$ be the finite field with q elements. Let m, n, r be positive integers. A polynomial of the form $L(Z) = \sum_{i=0}^{r} a_i Z^{q^i} \in \mathbb{F}_{q^m}[Z]$ is called a linearized polynomial. This type of polynomials is particularly important in coding theory, specifically for the theory of rank-metric codes, where they are used to construct a fundamental family of maximum rank-distance (MRD) codes, called Gabidulin codes. Linearized polynomials are also deeply connected to Drinfeld module's theory and recently, as shown in [1], such connection has been used to construct a new infinite family of optimal rank-metric codes with rank-locality, improving some previous parameters and divisibility conditions present in the construction of [3]. Therefore, it comes natural to investigate properties of linearized polynomials in more depth and in terms of Drinfeld modules. An obvious property is that each linearized polynomial can be seen as an $\mathbb{F}_q$-linear map, and so it makes sense to talk about the characteristic polynomial of a linearized polynomial. In this talk, we show how the theory of Drinfeld modules, together with the theory of linear recurrence sequences, can be used to compute the characteristic polynomial $C_L^{(n)}$ of the $\mathbb{F}_q$-linear map associated

to a linearized polynomial $L \in \mathbb{F}_{q^m}[Z]$ acting on an extension $\mathbb{F}_{q^{mn}}$ of $\mathbb{F}_{q^m}$. Then, we provide a new algorithm to compute $C_L^{(n)}$, and we show that its running time is $O(n\log^2(n))$ in terms of $\mathbb{F}_q$ operations. This means that, when $n \gg 0$, our algorithm outperforms any other standard algorithm known in literature, since they instead have a running time of $O(n^\omega \log(n))$ where $2 \leq \omega \leq 3$ (see for example [4] **??**).
This is a joint work with Giacomo Micheli and Shujun Zhao.

References

[1] Luca Bastioni, Mohamed O. Darwish, Giacomo Micheli. Optimal Rank-Metric Codes with Rank-Locality from Drinfeld Modules. *arXiv:2407.06081*, 2024.

[2] Ran Duan, Hongxun Wu, Renfei Zhou. Faster matrix multiplication via asymmetric hashing. In *2023 IEEE 64th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 2129–2138, 2023.

[3] Swanand Kadhe, Salim El Rouayheb, Iwan Duursma, Alex Sprintson. Rank-metric codes with local recoverability. In *54th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*. IEEE, Sept. 2016.

[4] Walter Keller-Gehrig. Fast algorithms for the characteristics polynomial. *Theoretical computer science*, 36:309–317, 1985.

[5] Clément Pernet, Arne Storjohann. Faster algorithms for the characteristic polynomial. In *Proceedings of the 2007 international symposium on Symbolic and algebraic computation*, pages 307–314. Association for Computing Machinery, 2007.

[6] Vincent Neiger, Clément Pernet. Deterministic computation of the characteristic polynomial in the time of matrix multiplication. *Journal of Complexity*, 67:101572, 2021.

17.7 Towards the classification of scattered binomials

Francesco Ghiandoni
University of Perugia, Italy

Joint work with Daniele Bartoli, Alessandro Giannoni and Giuseppe Marino.

Let f be an $\mathbb{F}_q$-linear function over $\mathbb{F}_{q^n}$. If $U = \{(x, f(x)) : x \in \mathbb{F}_{q^n}\}$ defines a maximum scattered $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^n} \times \mathbb{F}_{q^n}$, f is said to be a scattered polynomial. So far, very few examples of such polynomials are known for each value of n and q. In particular, the only known families of scattered binomials are

(LP) $f(x) = \delta x^{q^s} + x^{q^{n-s}}$, with $\gcd(s, n) = 1$ and $\delta^{(q^n-1)/(q-1)} \neq 1$;

(CMPZ) $f(x) = \delta x^{q^s} + x^{q^{n/2+s}}$, for $n = 6, 8$ and certain choices of δ.

In this talk, we will show that, at least when n is a prime integer, scattered binomials are of LP type only. Finally, a classification of scattered binomials over $\mathbb{F}_{q^n}$ for $n \leq 8$ is exhibited.

References

[1] D. Bartoli, B. Csajbók, M. Montanucci. On a conjecture about maximum scattered subspaces of $\mathbb{F}_{q^6} \times \mathbb{F}_{q^6}$, *Linear Algebra Appl.*, **631**:111–135, 2021.

[2] B. Csajbók, G. Marino, O. Polverino, C. Zanella. A new family of MRD-codes, *Linear Algebra Appl.*, **548**:203–220, 2018.

[3] G. Lunardon, R. Trombetti, Y. Zhou. Generalized twisted Gabidulin codes, *J. Combin. Theory Ser. A*, **159**:79–106, 2018.

[4] J. Sheekey. A new family of linear maximum rank distance codes, *Adv. Math. Commun.*, **10**(3):475–488, 2016.

[5] M. Timpanella, G. Zini. On a family of linear MRD codes with parameters $[8 \times 8, 16, 7]_q$. *Des. Codes Cryptogr.* , **92**(3):507–530, 2024.

17.8 The geometry of one-weight linear rank-metric codes

Alessandro Neri
University of Naples Federico II, Italy

A one-weight code is an error-correcting code in which all the nonzero codewords have the same weight. In 1984, Bonisoli provided a classification of one-weight linear codes by leveraging the connection between codes equipped with the Hamming metric and projective systems, which represent their geometric counterparts. More recently, similar geometric techniques have been applied to the study of codes in the rank metric with maximum left idealizer. In this talk, we discuss general one-weight linear rank-metric codes without any further assumption. This is done by exploiting a new geometric framework based on the tensor representation of linear rank-metric codes. This is a joint work with Gianira N. Alfarano and Martino Borello.

17.9 Codes deriving from some subvarieties of the Segre variety

Valentina Pepe
Sapienza University of Rome, Italy

Let $\mathbb{K}$ be the Galois field $\mathbb{F}_{q^t}$ of order q^t, $q = p^e$, p a prime, $A = Aut(\mathbb{K})$ be the automorphism group of $\mathbb{K}$ and $\boldsymbol{\sigma} = (\sigma_0, \dots, \sigma_{d-1}) \in A^d$, $d \geq 1$. The following generalization of the Veronese map is studied:

$$v_{d,\boldsymbol{\sigma}} : \langle v \rangle \in \mathrm{PG}(n-1, \mathbb{K}) \longrightarrow \langle v^{\sigma_0} \otimes v^{\sigma_1} \otimes \cdots \otimes v^{\sigma_{d-1}} \rangle \in \mathrm{PG}(n^d - 1, \mathbb{K}).$$

We investigate the link between such points sets and a linear code $\mathcal{C}_{d,\boldsymbol{\sigma}}$ that can be associated to the variety, obtaining examples of MDS and almost MDS codes.

This is a joint work with N. Durante and G. Longobardi.

References

[1] N. Durante, G. Longobardi, V. Pepe. $(d, \boldsymbol{\sigma})$-Veronese variety and some applications *Des. Codes Cryptogr.*, 91:1911–1921, 2023.

17.10 Quantum LDPC codes and decoding challenges

Tefjol Pllaha
University of South Florida, USA

Quantum Low-Density Parity-Check codes are promising candidates for scalable, fault-tolerant quantum computing. Represented by sparse parity check matrices, these codes share challenges with their classical counterparts —iterative decoding can fail to converge, may converge to an erroneous estimate, or return degenerate errors. In this talk, we will examine the structure of failure inducing sets (sets of nodes that, when initially in error, result in a decoding failure), and how the chosen graph representation may affect the presence of these sets.

17.11 Lattices over Non-Archimedean Fields and Their Applications to Coding Theory

Michael Schaller
University of Zurich, Switzerland

In this talk we will introduce lattices over non-archimedean fields following the work of Mahler [1] and Lenstra [2]. Welch and Scholtz [3] showed that the Berlekamp-Massey algorithm is closely related to continued fractions over the rational function field. It is well known for the real numbers that continued fractions are closely related to lattices. We will reinterpret the article of Welch and Scholtz in terms of lattice reduction over non-archimedean fields and then we will explore the work of Cohn and Heninger [4] on list decoding from the lattice point of view.

References

[1] K. Mahler. An analogue to Minkowski's geometry of numbers in a field of series. Annals of Mathematics, 42, 1941.
[2] A. K. Lenstra. Factoring multivariate polynomials over finite fields. Proceedings of the fifteenth annual ACM symposium on Theory of computing, 1983.
[3] L. Welch, and R. Scholtz. Continued fractions and Berlekamp's algorithm. IEEE Transactions on Information Theory, 1979
[4] H. Cohn, and N. Heninger. Ideal forms of Coppersmith's theorem and Guruswami-Sudan list decoding. Advances in Mathematics of Communications, 2015, `http://arxiv.org/abs/1008.1284`,

17.12 On the minimum weight of some geometric codes

Rocco Trombetti
University of Naples Federico II, Italy

(A joint work with: Bence Csajbók, Giovanni Longobardi and Giuseppe Marino)

Assume p is a prime and m, h are two positive integers. Let $\Sigma = \mathrm{PG}(m, q)$ be the m-dimensional projective space over the Galois field $\mathbb{F}_q$ where $q = p^h$, and denote by the symbol $\mathcal{D}_\Sigma(m, q)$ the $2-(v, q+1, 1)$ design of points and lines of Σ; hence, with $v = \frac{q^{m+1}-1}{q-1}$. The p-ary code $\mathcal{C} = \mathcal{C}_\Sigma(m, q)$ associated with such a design is the $\mathbb{F}_p$-subspace generated by the incidence vectors of the blocks of the corresponding design. Also, the dual $\mathcal{C}^\perp$ of $\mathcal{C}$ is the $\mathbb{F}_p$-subspace of vectors of $\mathbb{F}_q^v$ which are orthogonal to all vectors of $\mathcal{C}$ (under the standard inner product). These are particular examples of so called *geometric codes*.

Unlike for codes derived from the designs of points and subspaces of Σ, the situation regarding the minimum weight of geometric codes is not as clear, and therefore its study is more challenging. In [3] the authors reduced this problem to the above mentioned case of points and lines of a projective space of suitable dimension. In [1] Bagchi and Inamdar proven that the minimum weight of $\mathcal{C}_\Sigma^\perp(m, q)$ is bounded from below by the value $2\left(\frac{q^m-1}{q-1}\left(1-\frac{1}{p}\right)+\frac{1}{p}\right)$.

This type of problem in coding theory can be quite naturally translated into one concerning with the cardinality of sets or *multi-sets* of points in projective or affine space with special intersection properties with respect to certain subspaces, as shown for instance in [2]. Using this geometrical approach and exploiting properties of certain kind of polynomial, in this talk, we will show a significant improvement of the bound stated in 2002 by Bagchi and Inamdar, in the case when $h > 1$, and $m, p > 2$.

References

[1] B. Bagchi, S. P. Inamdar. Projective geometric codes. J. Combin. Theory Ser. A, 99(1) (2002), 128–142.

[2] Ball, A. Blokhuis, A. Gács, P. Sziklai, Zs. Weiner. On linear codes whose weights and length have a common divisor. Adv. Math., 211 (2007) 94–104.

[3] M. Lavrauw, L. Storme, G. Van de Voorde. On the code generated by the incidence matrix of points and k-spaces in PG(n, q) and its dual. Finite Fields Appl., 14(4) (2008), 1020-1038.

SPECIAL SESSION 18

Noncommutative Symbolic Computation

Symbolic computation plays an important role in the study of many important functions and their special values. By constructing noncommutative formal series based on words using these symbols, one can often discover key properties of these functions and values in a uniform way. On the other hand, noncommutative formal series can be considered as a generalization of language theory in theoretical computer science. As the algorithms and combinatorics of these series is based on those of words, these two fields naturally reinforce each other. They form an ideal framework for developing software based on computer algebra systems with rigor and efficiency. In particular, they allow the symbolic manipulation of several classes of special functions (such as Eulerian functions, hypergeometric functions, hyperlogarithms, harmonic sums, etc.) and of special values involved in solutions of differential equations. We invite contributions with the following topics:

- Combinatorial Indexing and Calculus
- Ecalle's Mould Calculus
- Free Lie Algebras
- Hopf Algebras and Their Combinatorics
- Noncommutative Differential Equations
- Multiple Zeta Values (or Zeta Polymorphism) and Polylogarithms
- Representative functions (Sweedler's duals and their combinatorics)

Session organizers

- Gérard H.E. Duchamp (Sorbonne University - Paris Nord, France)
- Vincel Hoang Ngoc Minh (University of Lille, France)
- Hiroaki Nakamura (Osaka University, Japan)
- Jianqiang Zhao (The Bishop's School, USA)

18.1 Various products of representative series and some applications

Van Chien BUI
University of Sciences, Hue University, Vietnam

Special functions such as polyzetas, multiple harmonic sums and polylogarithms are defined over $\mathcal{H}_r := \{(s_1, \ldots, s_r) \in \mathbb{N}_{\geq 1}^r, s_1 > 1\}$. Polyzetas values are given by the formula:

$$\zeta(s_1, \ldots, s_r) = \sum_{n_1 > \ldots > n_r > 0} n_1^{-s_1} \ldots n_r^{-s_r}, \tag{18.1}$$

polylogarithms (denoted $(Li_{s_1,\ldots,s_r})$ with $s_j \geq 1, r \geq 1$) and multiple harmonic sums (denoted $(H_{s_1,\ldots,s_r})$ with $s_j \geq 1, r \geq 1$). They are defined as follows (with $n \in \mathbb{N}_{\geq 1}$):

$$Li_{s_1,\ldots,s_r}(z) = \sum_{n_1 > \cdots > n_r > 0} n_1^{-s_1} \ldots n_r^{-s_r} z^{n_1} \tag{18.2}$$

and

$$H_{s_1,\ldots,s_r}(n) = \sum_{n \geq n_1 > \cdots > n_r > 0} n_1^{-s_1} \ldots n_r^{-s_r}. \tag{18.3}$$

They are compatible with algebraic structures of quasi-shuffle products, in some different cases of the parameter q:

$$u \sqcup\!\sqcup 1_{Y^*} = 1_{Y^*} \sqcup\!\sqcup u = u, \quad y_i u \sqcup\!\sqcup y_j v = y_i(u \sqcup\!\sqcup y_j v) + y_j(y_i u \sqcup\!\sqcup v) + q y_{i+j}(u \sqcup\!\sqcup v), \tag{18.4}$$

where ε is the empty word, y_i, y_j, y_{i+j} are letters of the alphabet $Y = \{y_k\}_{k \in \mathbb{N}_{\geq 1}}$, and u, v are words in the monoid Y^*.

For a commutative ring A containing the field of rational numbers $\mathbb{Q}$, we examine the set of noncommutative formal series, denoted by $A\langle\langle \mathcal{X} \rangle\rangle$. Within this set, representative series, that are closed under various products, form a module. This is a central focus of our research.

In this presentation, we will delve into how to factorize and decompose these noncommutative rational series and explore their relevance to theoretical computer science.

References

[1] Bui, V. C., Duchamp, G., Hoang Ngoc Minh, V., Ladji, K. & Tollu, C. Dual bases for noncommutative symmetric and quasi-symmetric functions via monoidal factorization. *J. Symbolic Comput.*. **75** pp. 56-73 (2016), `http://dx.doi.org/10.1016/j.jsc.2015.11.007`

[2] Bui, V. C., Duchamp, G. & Hoang Ngoc Minh, V. Schützenberger's factorization on the (completed) Hopf algebra of q-stuffle product. *JP J. Algebra Number Theory Appl.*. **30**, 191-215 (2013)

[3] Bui, V. C., Duchamp, G. & Hoang Ngoc Minh, V. Structure of Polyzetas and Explicit Representation on Transcendence Bases of Shuffle and Stuffle Algebras. *P. Symposium On Symbolic And Algebraic Computation.* **40**, 93-100 (2015)

[4] Bui, V. C., Duchamp, G. & Hoang Ngoc Minh, V. Computation tool for the q-deformed quasi-shuffle algebras and representations of structure of MZVs. *ACM Commun. Comput. Algebra.* **49**, 117-120 (2015)

[5] Bui, V. C., Duchamp, G. & Hoang Ngoc Minh, V. Structure of polyzetas and explicit representation on transcendence bases of shuffle and stuffle algebras. *J. Symbolic Comput.*. **83** pp. 93-111 (2017), `https://doi.org/10.1016/j.jsc.2016.11.007`

[6] Bui, V. C., Duchamp, G., Ngô, Q., Hoang Ngoc Minh, V. & Tollu, C. (Pure) transcendence bases in φ-deformed shuffle bialgebras. *Sém. Lothar. Combin.*. **74** pp. Art. B74f, 22

[7] Chien, B., Duchamp, G., Minh, H., Tollu, C. & Nghia, N. Combinatorics of φ-deformed stuffle Hopf algebras. *CoRR.* **abs/1302.5391** (2013), http://arxiv.org/abs/1302.5391
[8] Cartier, P. Fonctions polylogarithmes, nombres polyzêtas et groupes pro-unipotents. *Astérisque.*, Exp. No. 885, viii, 137-173 (2002), Séminaire Bourbaki, Vol. 2000/2001
[9] Cartier, P. Jacobienne généralisées, monodromie unipotente et intégrales intérées. *Séminaire BOURBAKI.* pp. 31-52 (1987)
[10] Cartier, P. Fonctions polylogarithmes, nombres polyzetas et groupes pro-unipotents. *Séminaire BOURBAKI.* **53**
[11] Drinfel'd, V. Quasi-Hopf algebras. *Algebra I Analiz.* **1**, 114-148 (1989)
[12] Drinfel'd, V. On quasitriangular quasi-Hopf algebras and on a group that is closely connected with Gal($\overline{Q}$/ Q). *Algebra I Analiz.* **2**, 149-181 (1990)
[13] Kleene, S. Representation of events in nerve nets and finite automata. *Automata Studies.* pp. 3-41 (1956)

18.2 Extension by continuity of the domain of Poly- and Hyperlogarithms

Gérard H.E. Duchamp
IHP and LIPN, Paris Sorbonne City, France

Motivated by the continuation of polylogarithms which is better understood through (improper) iterated integrals and noncommutative differential equations (with asymptotic initial condition), we extend by continuity the initial domain of indexation of Poly- (and Hyper-) logarithms. Remarking that the codomain of the Li arrow is a nuclear space, we observe that this new domain is a shuffle subalgebra of the algebra of noncommutative series. This method can be applied *mutatis mutandis* to hyperlogarithms. If time permits, we give further insights and applications in particular by substitution of remarkable representative series.

18.3 Various bialgebras of representative functions on free monoids

V. Hoang Ngoc Minh
University of Lille, France

Factorization and decomposition of representative functions with values in a (commutative) ring A and on a free monoid $\mathcal{X}^*$, generated by an (infinite or infinite) alphabet $\mathcal{X}$, are equivalent to factorization and decomposition of their graphs, viewed as noncommutative rational series admitting linear representations.

To factorize and to decompose these graphs we examine various products (as concatenation, shuffle and its commutative ϕ-deformations) of noncommutative series (over $\mathcal{X}^*$ with values in A) and coproducts which are such that their associated non graded bialgebras, on a field K, are isomorphic to the Sweedler's dual of the graded noncommutative co-commutative K-bialgebra of polynomials having only Kleene stars of the plane as characters, for concatenation. Moreover, the A-subalgebra of Kleene stars of the plane is closed by these various products.

18.4 Families of eulerian functions involved in regularization of divergent polyzetas

Ngo Quoc Hoan

Hanoi University of Science and Technology, Viet Nam

For any $r \in \mathbb{N}_{\geq 1}$ and $(s_1, \ldots, s_r) \in \mathbb{C}^r$, let us consider the following *several variable zeta function* (polyzetas) [3] $\zeta(s_1, \ldots, s_r) := \sum_{n_1 > \ldots > n_r > 0} n_1^{-s_1} \ldots n_r^{-s_r}$ which converges for $(s_1, \ldots, s_r)$ in the open sub-domain of $\mathbb{C}^r$ [2] and [6], $\mathcal{H}_r := \{(s_1, \ldots, s_r) \in \mathbb{C}^r \,|\, \forall m = 1, \ldots, r, \sum_{i=1}^{m} \mathrm{Re}(s_i) > m\}$. From Weierstrass factorization and Newton-Girard identity [3] and [4], one has successively

$$\frac{1}{\Gamma(z+1)} = e^{\gamma z} \prod_{n \geq 1} \Big(1 + \frac{z}{n}\Big) e^{-\frac{z}{n}} = \exp\Big(\gamma z - \sum_{k \geq 2} \zeta(k) \frac{(-z)^k}{k}\Big) \tag{18.5}$$

where $\Gamma(z)$ defines the Gamma function. One can deduce the following expression for $\zeta(2k)$:

$$\frac{\zeta(2k)}{\pi^{2k}} = k \sum_{l=1}^{k} \frac{(-1)^{k+l}}{l} \sum_{\substack{n_1, \ldots, n_l \geq 1 \\ n_1 + \ldots + n_l = k}} \prod_{i=1}^{l} \frac{1}{\Gamma(2n_i + 2)} \in \mathbb{Q}. \tag{18.6}$$

The formula (18.6) is a different version of a result of L. Euler using Bernoulli numbers

$$\frac{\zeta(2k)}{\pi^{2k}} = \frac{(-1)^{k+1} 2^{2k-1} B_{2k}}{(2k)!}, \; k \in \mathbb{N}.$$

In this talk, based on the combinatorics of noncommutative generating series, we discuss a way to extend the formula (18.5) and then we present a recurrence relation of $\zeta(2^k, \ldots, 2^k), \; k \in \mathbb{N}^*$. This is based on join works with Prof. Hoang Ngoc Minh and Prof. Gérard Duchamp [4].

References

[1] Jean Dieudonné, *Infinitesimal calculus*, Houghton Mifflin, 1971.
[2] A.B. Goncharov, *Multiple polylogarithms and mixed Tate motives*, 2001.
[3] V. Hoang Ngoc Minh, *Summations of Polylogarithms via Evaluation Transform*, in Math. & Comp. in Simul., 1336, p. 707-728, 1996.
[4] Bui Van Chien, Hoang Ngoc Minh, Ngo Quoc Hoan, Nguyen Dinh Vu, *Families of eulerian functions involved in regularization of divergent polyzetas*, Pub. Math. de Besancon, p. 5-28, 2023.
[5] A. Lascoux, *Fonctions symétriques*, SLC, B08e, 1983.
[6] J. Zhao, *Analytic continuation of multiple zeta functions*, Proc. A. M. S., 128 (5), p. 1275 - 1283, 1999.

18.5 Unramified Variants of Motivic Multiple Zeta Values

Jianqiang Zhao
The Bishop's School, USA

In this talk we shall consider a few variants of the motivic multiple zeta values of level two by restricting the summation indices in the definition of multiple zeta values to some fixed parity patterns. These include Hoffman's multiple t-values, Kaneko and Tsumura's multiple T-values, and the multiple S-values studied previously by Prof. Ce XU and the speaker. We will explain how to use Brown and Glanois's descent theory to determine some ramified and unramified families of motivic versions of these values. Assuming Grothendieck's period conjecture, our results partially confirm a conjecture of Kaneko and Tsumura about when multiple T-values can be expressed as a rational linear combination of multiple zeta values (i.e., unramified) if their depth is less than four. We will propose some unsolved problems at the end of the talk. This is a joint work with Prof. C. Xu.

18.6 A combinatorial property of multiple polylogarithms at non-positive indices

K. Kitamura
University of Osaka, Japan

The (double) shuffle relations for multiple polylogarithms at positive indices are well-known and have very beautiful properties. On the other hand, there are some analogy such as [1],[2] and [3] for MPL at non-positive (or general) indices. In this talk, we will show a new formula on products of MPL at non-positive indices in view of [4], and we will give some applications.

References

[1] G. H. E. Duchamp, V. H. N. Minh, Q. H. Ngo, Harmonic sums and polylogarithms at non-positive multi indices, *Journal of Symbolic Computation*, **83**(2017)166-186, 2016, https://doi.org/10.1016/j.jsc.2016.11.010.

[2] G. H. E. Duchamp, V. H. N. Minh, Q. H. Ngo, K. A. Penson, P. Simonnet, Mathematical renormalization in quantum electrodynamics via noncommutative generating series, *Applications of computer algebra*, 59–100, 2017, https://doi.org/10.48550/arXiv.1702.08550.

[3] Ebrahimi-Fard, Kurusch and Manchon, Dominique and Singer, Johannes, The Hopf Algebra of (q-)Multiple Polylogarithms with Non-positive Arguments, *International Mathematics Research Notices*, **16**(2017) 4882-4922, 2016, https://doi.org/10.48550/arXiv.1503.02977.

[4] H. Nakamura, Demi-shuffle duals of Magnus polynomials in a free associative algebra, *Algebraic Combinatroics*, **6**(2023) no.4 929-939, 2021, https://doi.org/10.5802/alco.287.

18.7 On Kashiwara-Vergne Lie algebra and double shuffle Lie algebra in mould theory

Nao Komiyama
Osaka University, Japan

In 2012, Schneps ([6]) showed that there exists an embedding between the double shuffle Lie algebra introduced by Racinet ([4]) and the Kashiwara-Vergne Lie algebra introduced by Alekseev and Torossian ([1]). In the proof of this embedding, a relation called the *senary relation* is used, which is a notion introduced in Ecalle's study ([2]) of multiple zeta values using mould theory. On Lie algebras and embeddings above, bigraded or elliptic versions have also been studied ([3], [5]). In my talk, I will explain the above topics and recent topic ([7]) as much as time permits.

References

[1] A. Alekseev and C. Torossian, The Kashiwara–Vergne conjecture and Drinfeld's associators, *Ann. Math.*, 175 (2012), no. 2, p. 415-463.

[2] J. Ecalle, The flexion structure and dimorphy: flexion units, singulators, generators, and the enumeration of multizeta irreducibles, *Asymptotics in dynamics, geometry and PDEs. Generalized Borel summation. Vol. II*, 2011, p. 27-211.

[3] H. Furusho and N. Komiyama, Kashiwara-Vergne and dihedral bigraded Lie algebras in mould theory, *Ann. Fac. Sci. Toulouse Math*, (6) 32 (2023), no. 4, 655–725.

[4] G. Racinet, Doubles mélanges des polylogarithmes multiples aux racines de l'unité, *Publ. Math. Inst. Hautes Études Sci.*, No. 95 (2002), 185–231.

[5] E. Raphael and L. Schneps, On linearised and elliptic versions of the Kashiwara-Vergne Lie algebra, 2017, https://arxiv.org/abs/1706.08299v1.

[6] L. Schneps, Double shuffle and Kashiwara-Vergne Lie algebras, *J. Algebra 367*, 2012, p. 54-74.

[7] L. Schneps, The double shuffle Lie algebra injects into the Kashiwara-Vergne Lie algebra, 2025, https://arxiv.org/abs/2504.14293.

18.8 Multiple Divided Bernoulli Polynomials and Numbers

Olivier Bouillot
Gustave Eiffel University, France

This work defines multiple divided Bernoulli polynomials by solving a system of difference equations that generalizes the classical Bernoulli case. These polynomials are required to span an algebra whose product matches the M basis of *QSym*. Although not unique, an explicit and notable solution is constructed using the reflection equation for Bernoulli polynomials.

18.9 Goncharov's programme, and symmetries of weight 6 multiple polylogarithms

Steven Charlton
Max Planck Institute for Mathematics, Germany

Multiple polylogarithms $\mathrm{Li}_{k_1,\dots,k_d}(x_1,\dots,x_d)$ are a class of multi-variable special functions generalising the natural logarithm $\mathrm{Li}_1(x) = -\log(1-x)$. These functions appear in connection with K-theory, hyperbolic geometry, values of L-functions, mixed Tate motives, high-energy physic, and many other areas.

One of the main challenges in the study of MPL's revolves around understanding on how many variables a MPL (or 'interesting' combinations thereof) actually depend ("the depth"). It is well known, for example, that $\mathrm{Li}_{1,1}$ can already be expressed via Li_2, likewise $\mathrm{Li}_{1,1,1}$ can be expressed via Li_3. Goncharov gave a conjectural criterion ("the Depth Conjecture") to determine this, using the motivic coproduct, as part of his programme to investigate Zagier's Polylogarithm Conjecture on the special values of the Dedekind zeta function $\zeta_F(m)$.

I will give an overview of Goncharov's Depth Conjecture, and its implications. I will discuss what is currently known, including recent progress in weight 6. In particular, the conjecture predicts that a certain weight 6 function (essentially a small modification of $\mathrm{Li}_{4,1,1}(x,y,z)$) should satisfy the 6-fold dilogarithm symmetries $\lambda \mapsto \lambda^{-1}, 1-\lambda$ in each variable independently, modulo depth ≤ 2 terms.

I will then describe the computational background and tools involved in investigating and proving these symmetries. In particular, one has to consider many possible degenerations (to boundary components of $\mathfrak{M}_{0,n}$) of the Matveiakin-Rudenko quadrangular polylogarithm functional equations, to iteratively find weaker symmetries of $\mathrm{Li}_{4,1,1}$ and useful short identities. To investigate higher weight analogues will require a more structure approach and understanding of this degeneration process.

18.10 A generalization of Magnus duality

Vu NGUYEN DINH
University of Science and Technology of Hanoi, Viet Nam

Let X be the finite graded set $X = B + Z$ (where $B = \{b_1, \ldots, b_M\}$ and $Z = \{z_1, \ldots, z_N\}$) and $\mathbb{K}$ being a fixed ring. In this talk, we first review a Zinbiel bialgebra structure over the associative algebra $\mathbb{K}\langle X\rangle$ and its graded dual studied in [1], [2] and [5]. We then use the concept of the classical Lazard elimination to construct a $\mathbb{K}$-linear basis of $\mathbb{K}\langle X\rangle$ which is called Magnus basis [3]. As the main purpose, we will explain how to use these generalized bialgebra structures over $\mathbb{K}\langle X\rangle$ to provide combinatorial tools in order to obtain the duality of Magnus basis. We claim that the duality can be automatically approached to any graded set $X = B + Z$ where $B = \{b_\gamma\}_{\gamma\in\Gamma}$ and $Z = \{z_\lambda\}_{\lambda\in\Lambda}$ (Γ, Λ are nonempty index sets). In case $X = B + Z$ where $B = \{x_0\}$ and $Z = \{x_\lambda\}_{\lambda\in\Lambda}$ (Λ: a nonempty index set, for example $\mathbb{N}_+$), the Magnus duality was appeared in [4], Theorem 3.2 to derive a formula of Le-Murakami, Furusho type that expresses arbitrary coefficients of a group-like series $\mathcal{J} \in \mathbb{K}\langle\langle x_0, x_1\rangle\rangle$ in terms of the "regular" coefficients of $\mathcal{J}$ ([4], Theorem 4.1).

This is based on join works with Prof. Gerard Duchamp and Prof. Vincel Hoang Ngoc Minh [6].

References

[1] E. Burgunder, *A symmetric version of Kontsevich graph complex and Leibniz homology*, J. Lie Theory, 20 (1) : 127-165, 2010.

[2] J. L. Loday, *Generalized bialgebras and triples of operads*, Asterisque 320 (2008), x+116 pp.

[3] W. Magnus, A. Karass, D. Solitar, *Combinatorial Group Theory: Presentations of Groups in Terms of Generators and Relations*, Dover Publications (1976).

[4] H. Nakamura, *Demi-shuffle duals of Magnus polynomials in free associative algebra,* Algebraic Combinatorics, Volume 6 (2023) no. 4, pp. 929-939.

[5] M. P. Schüzenberger, *Sur une propriété combinatoire des algèbres de Lie libres pouvant être utilisée dans un problème de mathéatiques appliqués*, Séminaire Dubreil–Jacotin Pisot (Algèbre et théorie des nombres) (1958/59).

[6] Vu NGUYEN DINH, *Combinatorics of Lazard Elimination and Interactions*, These (2023), Université Sorbonne Paris Nord.

18.11 Multiplicative structure of some multivariate functions

Jean-Yves Enjalbert
Lycée Jean-Batiste Corort, France

We will examine various families of multivariate functions, including the well-known multivariate functions.

$$\zeta(s_1; \ldots; s_n) = \sum_{n_1>\ldots>n_r>0} \frac{1}{n_1^{s_1} \ldots n_r^{s_r}}$$

For each family, we propose an efficient coding on an alphabet X, and transfer the multiplicative laws of their algebras to the alphabet X using the ϕ-stuffle $\sqcup\!\sqcup_\phi$, defined recursively by:

$$\forall(a,b) \in X^2, \forall(u,v) \in (X^*)^2, \quad au\sqcup\!\sqcup_\phi vb = a(u\sqcup\!\sqcup_\phi bv) + b(au\sqcup\!\sqcup_\phi v) + \phi(a,b)(u\sqcup\!\sqcup_\phi v),$$

The following will be studied:

- the explanation of ϕ according to various contexts.
- the conditions on ϕ to benefit from Radford's theorem, i.e., having a transcendence basis on the algebra generated by the family considered. Note that the basis is given explicitly, with a construction method allowing an efficient implementation of the algebra.

- the conditions on ϕ to determine the possibility of dualizing the mixing law, and therefore of a Hopf algebra structure.

The study will conclude by returning to the families introduced in the introduction.