SCALE

Applications of Computer Algebra

ACA 2022

Program and Abstracts

GEBZE TECHNICAL UNIVERSITY

MATEMATİK TÜRKİYE

EDITORS

- Hadi Alizadeh
- Muhammed Ergen
- Aslıhan Gür
- Ilias Kotsireas
- Veronika Pillwein
- Michael Wester
- Zafeirakis Zafeirakopoulos

General Chair
Zafeirakis Zafeirakopoulos, Gebze Technical University, Turkey

Program Committee Chair
Veronika Pillwein, Johannes Kepler University, Linz, Austria

Advisory Committee
Ilias Kotsireas, Waterloo, Canada
Michael Wester, New Mexico, USA

Organizing Committee
Hadi Alizadeh
Tülay Ayyıldız
Fatma Karaoğlu
Hülya Öztürk
Dimitris E. Simos
Elias Tsigaridas
Ali Kemal Uncu

Local Committee
Muhammed Ergen
Ayten Gezici
Aslıhan Gür
Başak Karakaş
Büşra Karadeniz Şen
Fatih Yetgin
Şeyma Yaşar
GTÜ Bilgisayar Topluluğu
Türkiye Matematik Kulübü

Welcome to ACA'2022! This is the first ACA (Applications of Computer Algebra) conference that will have in-person attendance since the beginning of the SARS-CoV-2/COVID-19 pandemic. ACA'2021 was completely online, while this meeting is a hybrid of in-person and virtual appearances. Since ACA is not simply a conference series, but a community of friends, we rejoice in restarting in-person interactions this year.

This conference is the 27th ACA, a series started by Stanly Steinberg and myself in Albuquerque, New Mexico in 1995 and held every year since except for 2020. See the table below for a complete listing of the ACA series. I note that the Gebze meeting is the third ACA in Asia. This year, ACA is part of SCALE 2022 (Symbolic Computation: Algorithms, Learning, and Engineering), a gathering together of ACA'2022 and CASC'2022 (Computer Algebra in Symbolic Computing) along with three summer schools and two workshops related to computer algebra. Zafeirakis Zafeirakopoulos is the energetic general chair of SCALE, while Veronika Pillwein is the program chair for ACA, and both along with many others have done much to make for a successful conference!

This is the second year of the ACA-ERA (Early Researcher Award). Special thanks goes to Ilias Kotsireas, ACA working group co-chair along with me, who initiated this idea and encouraged funding from a number of sponsors. We hope this will establish a tradition of honoring and encouraging researchers early in their careers who are interested in computer algebra applications. We had some fine nominees this year and each one deserves recognition for their research and service to the community.

Thank you all very much for participating!

— Michael J. Wester

Conferences on Applications of Computer Algebra

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			2023	Warsaw, Poland

General Table

Times	MON – 08/15			TUE – 08/16			WED – 08/17			THU – 08/18			FRI – 08/19			Times
9:30-10:00	OPENING			S4	S5	S8	S1	S5	S8	S1	S6	S11	S1	S6	S3	9:30-10:00
10:00-10:30	S4	S14	S5													10:00-10:30
10:30-11:00										S5						10:30-11:00
coffee																CB
11:30-12:00	S4	S2	S9	Invited Talk			S1	S2	S8	Invited Talk			S2	S6		11:30-12:00
12:00-12:30													S15		S15	12:00-12:30
lunch																LB
14:00-14:30	S4	S5	S14	S9	S5	S11	S3	S13	S8	Excursion			S3	S6	S2	14:00-14:30
14:30-15:00																14:30-15:00
15:00-15:30													CLOSING			15:00-15:30
15:30-16:00																15:30-16:00
coffee																CB
16:30-17:00	S4	S13	S15	S6	S13	S11	S8	S5								16:30-17:00
17:00-17:30																17:00-17:30
17:30-18:00							Group Picture									17:30-18:00
18:00-18:30							ACA BM									18:00-18:30

S1–Computational Differential and Difference Algebra and its Applications Session

S2–Computer Algebra in Education Session

S3–Computer Algebra Modeling in Science and Engineering Session

S4–Effective Ideal Theory and Combinatorial Techniques in Commutative and non Commutative Rings and Their Applications Session

S5–Algorithmic and Experimental Combinatorics Session

S6–D-finite Functions and Beyond: Algorithms, Combinatorics, and Arithmetic Session

S8–Algebraic and Geometric Methods in Coding Theory Session

S9–Parametric Polynomial Systems Session

S11–q-Analogues in Combinatorics: Matroids, Designs and Codes Session

S13–Computer Algebra Applications in the Life Sciences Session

S14–Algorithms in Cryptography and Blockchain Session

S15–General Session

Schedule for Invited Talks

TIME	**TUESDAY–2022/08/16**
11:30	The discrete logarithm problem in finite fields *Cécile Pierrot*
	THURSDAY–2022/08/18
11:30	Computer Algebra and Satisfiability Modulo Theories *James H. Davenport*

Schedule for Computational Differential and Difference Algebra and its Applications Session (S1)

Organized by Alexander Levin, Alexey Ovchinnikov, and Daniel Robertz

TIME WEDNESDAY–2022/08/17

09:30 Computing rational first integrals of polynomial vector fields on surfaces
Thierry Combot

10:00 On normal forms in differential Galois theory for the classical groups
Matthias Seiß, Daniel Robertz

10:30 Generalized characteristic sets and a new type of multivariate difference dimension polynomials
Alexander Levin

11:30 Integrable cases of the autonomic polynomial system
Victor Edneral

12:00 Twisted Mahler discrete residues
Carlos E. Arreche, Yi Zhang

THURSDAY–2022/08/18

09:30 Reynolds algebras and their free objects by Gröbner-Shirshov bases
Xing Gao, Li Guo, Tianjie Zhang

10:00 Elimination of unknowns in dynamical systems
Antonio Jiménez-Pastor, Alexey Ovchinnikov, Sonia L. Rueda

FRIDAY–2022/08/19

09:30 Algorithmic detection of conserved quantities of finite-difference schemes using difference algebra
Diogo Gomes, Friedemann Krannich, Ricardo de Lima Ribeiro

10:00 Holonomic modules and 1-generation in the Jacobian Conjecture
Vladimir Bavula

10:30 Computing the exceptional parameter set for a family of linear differential equations
Ruyong Feng, Michael Wibmer

Schedule for Computer Algebra in Education Session (S2)

Organized by Michel Beaudin, Michael Wester, Noah Dana-Picard, Alkis Akritas, José Luis Galán García, and Elena Varbanova

TIME	**MONDAY–2022/08/15**
11:30	Computer Algebra Systems – powerful tools for creating teaching-learning resources in undergraduate mathematics *E. Varbanova*
12:00	Using CAS in theclassroom: personal thought (Part II) *M. Beaudin*

	WEDNESDAY–2022/08/17
11:30	Simplified models of planetary orbits, virtual space mandalas and beyond *T. Dana-Picard*

	FRIDAY–2022/08/19
11:30	Comprehensive solutions to problems in Maple, using the parametric option *D. J. Jeffrey*
14:00	Multivalued functions and cubic equations *V. M. Quance, M. R. Vancea, D. J. Jeffrey*

Schedule for Computer Algebra Modeling in Science and Engineering Session (S3)

Organized by Alexander Prokopenya and Haiduke Sarafian

TIME	**WEDNESDAY–2022/08/17**
14:00	Designing physics problems with Mathematica: Example I *H. Sarafian*
14:30	Designing physics problems with Mathematica: Example II *H. Sarafian*
15:00	Photoelastic and numerical stress analysis of a pin on a plan contact subjected to a normal and a tangential load *M. Beldi, A. Bilek*
15:30	Numerical and experimental analysis of stress fields in mechanical contacts between solids (rigid/deformable and deformable/deformable) *M. Beldi, A. Bilek*

	FRIDAY–2022/08/19
09:30	Discrete models of epidemic spread in a heterogeneous population *M. Choiński, M. Badzioch, U. Foryś*
10:00	Fitting sparse reduced data *R. Kozera*
10:30	Resonances and periodic motion of Atwood's machine with two oscillating bodies *A. Prokopenya*
14:00	Perturbations in the restricted three-body problem of variable masses *A. Prokopenya, M. Minglibayev, A. Ibraimova*
14:30	Evolutionary equations of the two-planet three-body problem with variable masses *A. Prokopenya, M. Minglibayev, A. Ibraimova*

Schedule for Effective Ideal Theory and Combinatorial Techniques in Commutative and non Commutative Rings and Their Applications Session (S4)

Organized by Michela Ceria, André Leroy, Samuel Lundqvist, and Teo Mora

TIME	MONDAY–2022/08/15
10.00	Generalized weights of codes via graded Betti numbers *Elisa Gorla*
11.30	Faster Change of Order Algorithm for Gröbner Bases Under Shape and Stability Assumptions *Jérémy Berthomieu, Vincent Neiger, Mohab Safey El Din*
12.00	Gröbner Bases and Tate Algebras of Varying Radii *Xavier Caruso, Tristan Vaccon, Thibaut Verron*
14:00	Duality, Trace Inversion Formula and Extreme Combinatorics: Yet another proof of Perles-Sauer-Shelah Lemma *Luis M.Pardo*
14:30	Solving degree and last fall degree *Alessio Caminata, Elisa Gorla*
15:00	Noncommutative Novikov algebras *Pavel Kolesnikov*
15:30	Discrete Vector Fields for Monomial Resolutions *Eduardo Sáenz-de-Cabezón, Francis Sergeraert*
16:30	Round table - discussions
17:00	Private Distributed Coded Computation *Malihe Aliasgari, Yousef Nejatbakhsh*
17:30	Algebraic, Geometric, and Combinatorial Aspects of Unique Model Identification *Brandilyn Stigler*
18:00	On computing isomorphisms between algebraic number fields *Michael Monagan*

	TUESDAY–2022/08/16
09:30	Linear Label Code of a Lattice Using Gröbner bases *Malihe Aliasgari, Daniel Panario, Mohammad-Reza Sadeghi*
10:00	On Toric Resolutions of Rational Singularities *Büşra Karadeniz Şen*
10:30	Sum of Disjoint Products approach to System Reliability based on Involutive Divisions *Rodrido Iglesias, Patricia Pascual-Ortigosa, Eduardo Sáenz-de-Cabezón*

Schedule for Algorithmic & Experimental Combinatorics Session (S5)

Organized by Miklos Bona, Ilias Kotsireas, and Ali K. Uncu

TIME	**MONDAY–2022/08/15**
10:00	Searching for Kochen–Specker systems with orderly generation and satisfiability solving *Curtis Bright, Zhengyu Li, Vijay Ganesh*
10:30	Counting points of modular curves over finite fields *Valerio Dose, Pietro Mercuri, Claudio Stirpe*
14:00	Experimenting with Young Tableaux *Doron Zeilberger*
14:30	Schmidt type partitions *Ae Ja Yee*
15:00	The Factorial-Basis Method for Finding Definite-Sum Solutions of Linear Recurrences *Antonio Jimenez-Pastor*
15:30	Regular languages and the enumeration of permutation classes *Vince Vatter*

	TUESDAY–2022/08/16
09:30	Well-Indumatched Pseudoforests *Yasemin Büyükçolak, Didem Gözüpek, Sibel Özkan*
10:00	Counting Labelled Trees of Certain Families *Emre Yivli, Emrah Akyar, Handan Akyar*
10:30	On the Directed Hamilton-Waterloo Problem with Uniform Cycle Sizes *Fatih Yetgin, Uğur Odabaşı, Sibel Özkan*
14:00	On generalizations of the third order mock theta functions $\omega(q)$ and $v(q)$ *Atul Dixit, Bruce Berndt, Rajat Gupta*
14:30	Linked partition ideals and computer algebra *Shane Chern*
15:00	Missing cases in parity considerations in Rogers–Ramanujan–Gordon type overpartitions *Kağan Kurşungöz, Mohammad Zadeh Dabbagh*
15:30	The Combinatorial Exploration Framework and its Consequences *Michael Albert, Christian Bean, Anders Claesson, Émile Nadeau, Jay Pantone, Henning Ulfarsson*

WEDNESDAY–2022/08/17

09:30 Partitions, Kernels, and the Localization Method
Nicolas Smoot

10:00 Combinatorial constructions of generating functions of cylindric partitions with small profiles into unrestricted or distinct parts
Kağan Kurşungöz, Halime Ömrüuzun Seyrek

10:30 Sum-of-tails Identities
Rajat Gupta

10:30 For *Hui Huang*'s talk please look the schedule of Computer Algebra Applications in the Life Sciences session

16:30 A Gessel Way to the Diagonal Theorem on D-finite Power Series
Shaoshi Chen, Pingchuan Ma, Chaochao Zhu

17:00 Factorizable systems of differential equations from particle physics: preprocessing and solving
Nikolai Fadeev

Schedule for D-finite Functions and Beyond: Algorithms, Combinatorics, and Arithmetic Session (S6)

Organized by Shaoshi Chen, Frederic Chyzak, Antonio Jimenez-Pastor, Manuel Kauers, and Veronika Pillwein

TIME	**TUESDAY–2022/08/16**
16:30	q-Difference Equation Systems for Cylindric Partition *Ali Uncu*
17:00	Series defined by quadratic differential equations *Bertrand Teguia Tabuguia*
17:30	Symbolic-Numeric Factorization of Differential Operators *Alexandre Goyer*
	THURSDAY–2022/08/18
9:30	Shift equivalence testing of polynomials and symbolic summation of multivariate rational functions *Lixin Du*
10:00	Arithmetic of polynomial dynamical systems *Mohammad Sadek*
10:30	Decision Problems for Second-Order Holonomic Recurrences *Eike Neumann*
	FRIDAY–2022/08/19
9:30	C^2 -finite Sequences: A Computational Approach *Philipp Nuspl*
10:00	Factoring differential operators in positive characteristic *Raphael Pages*
10:30	Working with DD-finite functions automatically on SageMath *Antonio Jiménez-Pastor*
11:30	Galois groups of linear difference-differential equations *Ruyong Feng*
12:00	Computing logarithmic parts by evaluation homomorphisms *Ziming Li*
14:00	Efficient q-integer linear decomposition of multivariate polynomials *Hui Huang*
14:30	D-finiteness, rationality, and height *Jason P. Bell*

Schedule for Algebraic and Geometric Methods in Coding Theory Session (S8)

Organized by Alessandro Neri and Ferdinando Zullo

TIME	TUESDAY–2022/08/16
09:30	Computational classification of symplectic 4-dimensional semifields over finite fields *Michel Lavrauw, John Sheekey*
10:00	Divisible codes and few-weight codes in the rank metric *John Sheekey, Olga Polverino, Paolo Santonastaso, Ferdinando Zullo*
10:30	Construction of Subspace Codes using Evaluation *Joachim Rosenthal*

	WEDNESDAY–2022/08/17
09:30	Protograph-based LDPC codes with chordless short cycles and large minimum distance *Farzane Amirzade, Daniel Panario, Mohammad-Reza Sadeghi*
10:00	Ordered Covering Arrays and NRT-metric Covering Codes *Lucia Moura*
10:30	Better CRC Codes *Anton Betten*
11:30	Constructions of new matroids and designs over $\mathbb{F}_q$ *Eimear Byrne, Michela Ceria, Sorina Ionica, Relinde Jurrius, Elif Saçikara*
12:00	Critical Problem, q-Polymatroids and Rank-Metric Codes *Gianira N. Alfarano, Eimear Byrne*
14:00	On the geometry of $(q+1)$-arcs of $\mathrm{PG}(3,q)$, q even *Michela Ceria, Francesco Pavese*
14:30	Trifferent codes and affine blocking sets *Anurag Bishnoi, Dion Gijsiwijt, Jozefien D'haesleer, Aditya Potukuchi*
15:00	Cameron–Liebler type sets and completely regular codes *Morgan Rodgers*
15:30	Mutually Orthogonal Latin Squares based on e-Klenian polynomials *Jaime Gutierrez, Jorge Jimenez Urroz*
16:30	On Optimal Binary Linear Complementary Pair of Codes *Cem Güneri*
17:00	On LCP of 1-generator QC codes *Zohreh Aliabadi*

Schedule for Parametric Polynomial Systems Session (S9)

Organized by Katsusuke Nabeshima and Yosuke Sato

TIME	**MONDAY–2022/08/15**
11:30	A deterministic method for computing Bertini type invariants of parametric ideals *Shinichi Tajima, Katsusuke Nabeshima*
12:00	Imaginary projections: Complex versus real coefficients *Stephan Gardoll, Thorsten Theobald, Mahsa Sayyary Namin*

	TUESDAY–2022/08/16
14:00	Generic Gröbner basis of a parametric ideal and its application to a comprehensive Gröbner system *Katsusuke Nabeshima*
14:30	Comprehensive Gröbner systems over finite fields *Ryoya Fukasaku, Yasuhiko Ikematsu*
15:00	Implementation report on parametric absolute factorization of multi-variate *Kazuhiro Yokoyama*
15:30	Simplification of comprehensive Gröbner systems using disequalities *Yosuke Sato*

Schedule for q-Analogues in Combinatorics: Matroids, Designs and Codes Session (S11)

Organized by Gianira Alfarano, Michela Ceria, and Relinde Jurrius

TIME	TUESDAY–2022/08/16
14:00	An alternative for the q-matroid axiom (I4) *Michela Ceria, Relinde Jurrius*
14:30	The direct sum of q-matroids *Michela Ceria, Relinde Jurrius*
15:00	q-Matroids and Rank-Metric Codes *Gianira N. Alfarano, Eimear Byrne*
15:30	A Geometric Characterization of Near MRD Codes *Alessandro Neri*
16:30	q-analog of Sidon sets and linear sets *Vito Napolitano, Olga Polverino, Paolo Santonastaso, Ferdinando Zullo*
17:00	Independent Spaces of q-Polymatroids *Vito Napolitano, Olga Polverino, Paolo Santonastaso, Heide Gluesing-Luerssen, Benjamin Jany*
17:30	Categories of q-Matroids *Benjamin Jany, Heide Gluesing-Luerssen*
18:00	Round table - Discussion

	THURSDAY–2022/08/18
9:30	A q-analogue of Critical Theorem for polymatroids *Koji Imamura, Keisuke Shiromoto*
10:00	Shellability and homology of q-complexes associated to q-matroids *Sudhir Ghorpade*
10:30	Generalized rank weights and Betti numbers *Rakhi Pratihar*

Schedule for Computer Algebra Applications in the Life Sciences Session (S13)

Organized by AmirHosein Sadeghimanesh, Ali Kemal Uncu, Hamid Rahkooy, and Matthias Seiß

TIME	**MONDAY–2022/08/15**
16:30	Detecting and precluding toricity in reaction network theory *Elisenda Feliu, Oskar Henriksson*
17:00	Estimating Genomic Periodicities *Daniel Lichtblau*
17:30	Are generic bifurcations always generic on chemical reaction networks? *Nicola Vassena*
18:00	Stability analysis and Hopf bifurcations in a tumor growth model *Dániel András Drexler, Ilona Nagy, Valery G. Romanovski*

	TUESDAY–2022/08/16
16:30	The shape of the parameter region of multistationarity in reaction networks *Elisenda Feliu, Máté L. Telek*
17:00	Disaster Incident Analysis via Algebra Stories *Berina Celic, Bernhard Garn, Dimitris E. Simos*
17:30	Nondegenerate Andronov–Hopf bifurcations in a class of bimolecular mass-action systems (Part I) *Murad Banaji, Balázs Boros*
18:00	Nondegenerate Andronov–Hopf bifurcations in a class of bimolecular mass-action systems (Part II) *Murad Banaji, Balázs Boros*

	WEDNESDAY–2022/08/17
14:00	Polynomial Systems Theories in Biology *James H. Davenport*
14:30	Open problems in parameteric dynamical systems from life sciences *Alexey Ovchinnikov*
15:00	Algebraic sequence modelling for disaster management *Klaus Kieseberg, Bernhard Garn, Dimitris E. Simos*

	THURSDAY–2022/08/18
10:30	Efficient Rational Creative Telescoping *Mark Giesbrecht, Hui Huang, George Labahn, Eugene Zima*
-	Hui Huang's talk is from Algorithmic & Experimental Combinatorics session

Schedule for Algorithms in Cryptography and Blockchain Session (S14)

Organized by Oğuz Yayla, Ahmet Sınak, Hamid Rahkooy, and Matthias Seiß

TIME	**MONDAY–2022/08/15**
10:00	Algebraic Network Analysis for Anti-Money Laundering *Ceren Culha, Bernhard Garn, Dimitris E. Simos*
10:30	A General Version of Carlet's Construction of APN Functions *İlksen Acunalp Erleblebici, Oğuz Yayla*
14:00	Handover Authentication Protocols in Mobile Networks *Hakan Yıldırım, Murat Cenk*
14:30	A Three-Party Lattice-Based Hybrid PAKE Protocol with Anonymity *Kübra Seyhan, Sedat Akleylek*
15:00	A Lattice-based Group Signature Scheme with Applications in Blockchain *Meryem Soysaldı Şahin, Sedat Akleylek*
15:30	Two Post-Quantum Code-Based Cryptosystems *Sedat Akleylek, Ebubekir Aydoğmuş, Ahmet Sınak*

Schedule for General Session (S15)

Organized by Zafeirakis Zafeirakopoulos

TIME	**Monday–2022/08/15**
16:30	A Call for more Automata Theory in Sequential Combinatorial Testing *Ludwig Kampel, Manuel Leithner, Dimitris E. Simos*
	FRIDAY–2022/08/19
12:00	Computer Algebra, Student Assessment and Learning Data Analysis *David Smith, Stephen M. Watt*
12:00	Certified Hermite Matrices from Approximate Roots *Tülay Ayyıldız Akoğlu, Agnes Szanto*

Contents

Computational Differential and Difference Algebra and its Applications

Computer Algebra in Education

Computer Algebra Modeling in Science and Engineering

Effective Ideal Theory and Combinatorial Techniques in Commutative and non Commutative Rings and Their Applications

Algorithmic & Experimental Combinatorics

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

Algebraic and Geometric Methods in Coding Theory

Parametric Polynomial Systems

q-Analogues in Combinatorics: Matroids, Designs and Codes

Computer Algebra Applications in the Life Sciences

Algorithms in Cryptography and Blockchain

General Session

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
“Invited Talk”

The discrete logarithm problem in finite fields

Cécile Pierrot [Cecile.Pierrot@inria.fr]

Abstract: The security of currently deployed public key protocols in cryptography relies on the presumed hardness of problems often coming from number theory, such as factoring a large integer or solving the discrete logarithm problem in some groups.

In this talk I focus on discrete logarithms in finite fields. I explain what is a discrete logarithm and why cryptographers need them. I focus on the best currently known algorithms to solve the related problem, together with open questions in this area.

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
“Invited Talk”

Computer Algebra and Satisfiability Modulo Theories

James H. Davenport [J.H.Davenport@bath.ac.uk]

Since Erika Abraham’s seminal talk at ISSAC 2015, there has been fruitful interaction between the fields of Computer Algebra and Satisfiability Modulo Theories. This has been helped by the SCSC (Symbolic Computation and Satisfiability Checking) EU project and workshop series. But what are the lessons for both fields from this collaboration? The author sees several such. Firstly for computer algebra.

1) The importance of pragmatics as well as complexity theory. SAT is the quintessential NP-complete problem, but has many excellent solvers in practice. Conversely, Computer Algebra has historically looked at worst-case complexity, which makes sense in many contexts, but not all.

2) The importance of curated benchmark sets. Both the SAT community and the SMT community have such sets, but computer algebra by-and-large does not. Each author invents his own collection, borrowing those that are borrowable (and too often they are only published in PDF) and publishing those that will fit in a page limit, and possibly publishing the complete set on a private website.

3) The question of being fast on trivial examples. The usual SAT/SMT benchmarking does a lot of this, whereas Computer Algebra tends to focus on the difficult examples.

There are also lessons for SMT, especially as it asks more questions about finite fields (a major trend at SMT 2022).

1) Large finite fields are not a problem: computer algebra systems have efficient big number arithmetic, so large primes are easily implemented, and large powers of small primes are also feasible.

2) However the usual way of working in GF(q) is to add the polynomial $x^q - x$ (for every variable x). This can indeed be very expensive, but there are partial solutions.

3) Difficult NRA (Nonlinear Real Arithmetic) problems are genuinely hard, and the full might of Computer Algebra should be deployed.

A problem for both fields, but where the SMT community is probably more advanced, is the question of the accuracy of the systems. Both Computer Algebra and SMT systems are large, complex, and often multi-generational, systems.

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *"Computational Differential and Difference Algebra and its Applications"*

Computing rational first integrals of polynomial vector fields on surfaces

Thierry Combot[1] [thierry.combot@u-bourgogne.fr]

[1] Institut mathématiques de Bourgogne, Université de Bourgogne, Dijon, France

Consider an algebraic surface $\mathcal{S}$ defined by a prime ideal $\mathcal{I} \subset \mathbb{Q}[x, y, z_1, \dots, z_l]$, and a vector field X on the tangent of $\mathcal{S}$. If $\mathcal{S}$ projects properly on the x, y plane, X represents an algebraic vector field in x, y. A rational first integral of X is a rational function on $\mathcal{S}$ which is constant along the orbits of X. In [1], an algorithm is presented to find rational first integrals for polynomial vector fields in the plane up to degree N. In the surface case, two new difficulties arise: the field of first integrals of X is not always generated by a single element, and the notion of degree of a first integral is not well defined. A set of rational first integrals generating the field of first integral defines an application of $\mathcal{S}$ to a curve of genus g. We will define the notion of minimal rational first integral, a notion of degree, and prove that minimal rational first integral are those whose image curve is of maximal genus. Depending on the genus g, we will see that three possibilities arise:

- If $g = 0$, the field is generated by a single first integral with coefficients in at worst a quadratic extension.
- If $g = 1$, the field is generated by two first integrals with an elliptic algebraic relation.
- If $g \geq 2$, the image curve can be complicated but the degree of first integrals can be bounded.

For each case, we will present an algorithm to compute such rational first integral up to degree N in time $O(N^{\omega+1})$. Some significant differences with the planar case will arise depending on the homology of $\mathcal{S}$.

Keywords
First integrals, Curve parametrization, Poincaré problem

[1] ALIN BOSTAN, GUILLAUME CHÈZE, THOMAS CLUZEAU, AND JACQUES-ARTHUR WEIL, Efficient algorithms for computing rational first integrals and Darboux polynomials of planar polynomial vector fields. *Math. Comp.* 85(299):1393–1425 (2016)

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *Computational Differential and Difference Algebra and its Applications*

On Normal Forms in Differential Galois Theory for the Classical Groups

Matthias Seiß[1], ***Daniel Robertz***[2] [mseiss@mathematik.uni-kassel.de]

[1] Institut für Mathematik, Universität Kassel, D–34109 Kassel, Germany
[2] Lehrstuhl für Algebra und Zahlentheorie, RWTH Aachen University, D–52056 Aachen, Germany

In classical Galois theory there is the well-known construction of the general polynomial equation over $\mathbb{Q}$ with Galois group the symmetric group S_n. The coefficients of the general equation are (up to sign) the elementary symmetric polynomials in n indeterminates $x_1, \ldots, x_n$ over $\mathbb{Q}$. Every algebraic extension of $\mathbb{Q}$ defined by a polynomial $p(x)$ of degree n is obtained as a specialization by substituting the roots of $p(x)$ for $x_1, \ldots, x_n$ in the general equation.

In an analogous way a general linear differential equation with differential Galois group the general linear group $\mathrm{GL}_n(C)$ over an algebraically closed field C of characteristic zero is obtained as follows. Extend the linear action of $\mathrm{GL}_n(C)$ on the vector whose coordinates are differential indeterminates $y_1, \ldots, y_n$ to the differential field of rational functions $C\langle y_1, \ldots, y_n\rangle$. Introducing a new differential indeterminate Y and denoting by $w(y_1, \ldots, y_n)$ the Wronskian of $y_1, \ldots, y_n$, the general differential equation is given by

$$0 \;=\; Y^{(n)} + c_{n-1}Y^{(n-1)} + \ldots + c_0 Y \;:=\; \frac{w(Y, y_1, \ldots, y_n)}{w(y_1, \ldots, y_n)}. \tag{1}$$

In fact, $c_{n-1}, \ldots, c_0$ are differentially algebraically independent generators of the fixed field of $C\langle y_1, \ldots, y_n\rangle$ under $\mathrm{GL}_n(C)$ (and recall that the elementary symmetric polynomials are algebraically independent generators of the fixed field of $Q(x_1, \ldots, x_n)$ under S_n). Every Picard-Vessiot extension of a differential field F, with field of constants C, defined by a linear differential polynomial of order n is obtained as a specialization of (1) by substituting the linearly independent solutions $\eta_1, \ldots, \eta_n$ for $y_1, \ldots, y_n$. Generalizations to groups other than $\mathrm{GL}_n(C)$ were obtained in [1] and [2]. In all these cases the general differential equation involves n differential indeterminates over C (apart from Y).

Another approach to constructing general differential equations for the classical groups was presented in [4] and [5]. This approach combines the geometric structure of a classical group G of Lie rank l with Picard-Vessiot theory and involves only l differential indeterminates. More precisely, the construction starts with a differential field $C\langle \boldsymbol{v}\rangle$ generated by l differential indeterminates $\boldsymbol{v} = (v_1, \ldots, v_l)$ over C. The general extension field in this approach is a

Liouvillian extension $\mathcal{E}$ of $C\langle \boldsymbol{v}\rangle$ with differential Galois group a fixed Borel subgroup $B^-(C)$ of $G(C)$. As in the case of $\mathrm{GL}_n(C)$ we construct a fundamental matrix Y and define an action of $G(C)$ on it which will then induce an action on $\mathcal{E}$. Fixing a Chevalley basis of the Lie algebra $\mathfrak{g}$ of G, the defining matrix of $\mathcal{E}$ is chosen such that its conjugate by a representative $\overline{w}$ of the longest Weyl group element is the sum of the Cartan subalgebra, parametrized by $\boldsymbol{v}$, and the basis elements of the root spaces corresponding to the simple roots. Choosing a fundamental matrix $b \in B^-(\mathcal{E})$ generating $\mathcal{E}$ over $C\langle \boldsymbol{v}\rangle$, we can construct a matrix u in the maximal unipotent subgroup of $B^-(C\langle \boldsymbol{v}\rangle)$ such that the logarithmic derivative of $Y = u\overline{w}b$ is the matrix $A_G(\boldsymbol{s})$ constructed in [4] and [5]. The differential polynomials $\boldsymbol{s} = (s_1, \ldots, s_l)$ in $C\{\boldsymbol{v}\}$ are differentially algebraically independent over C. The matrix u is the product of matrices of root groups corresponding to all negative roots Φ^- and it depends on $|\Phi^-|$ differential polynomials $\boldsymbol{p}$ in $C\{\boldsymbol{v}\}$, those corresponding to the negative simple roots being the indeterminates $\boldsymbol{v}$. Multiplying Y from the right by an element of the full group $G(C)$ and then taking the Bruhat decomposition defines an action on $\boldsymbol{p}$ and on the generators of the Liouvillian extension, i.e. the entries of b, and therefore on $\mathcal{E}$. The fixed field under the induced action of $G(C)$ on $\mathcal{E}$ is $C\langle \boldsymbol{s}\rangle$ and it is shown that the extension $\mathcal{E}$ of $C\langle \boldsymbol{s}\rangle$ is a Picard-Vessiot extension with differential Galois group $G(C)$. The construction is only generic for Picard-Vessiot extensions of F with defining matrix gauge equivalent to a matrix in *normal form*, i.e. a specialization of $A_G(\boldsymbol{s})$. Deciding such a gauge equivalence is non-trivial as a consequence of the fact that $\mathcal{E}$ and $C\langle \boldsymbol{s}\rangle$ have differential transcendence degree l over C.

This talk is dedicated to the question of the genericity properties of the extension $\mathcal{E}$ over $C\langle \boldsymbol{s}\rangle$. We consider the problem of gauge equivalence of a generic element of the Lie algebra to a matrix in normal form. More precisely, let d be the dimension of the classical group G and let $\boldsymbol{a} = (a_1, \ldots, a_d)$ be differential indeterminates over a differential field F with constants C. Further let $A(\boldsymbol{a})$ be a generic element in the Lie algebra $\mathfrak{g}(F\langle \boldsymbol{a}\rangle)$ obtained from parametrizing the Chevalley basis from above with the indeterminates $\boldsymbol{a}$. It is known (cf. [3]) that the differential Galois group of $\boldsymbol{y}' = A(\boldsymbol{a})\boldsymbol{y}$ over $F\langle \boldsymbol{a}\rangle$ is $G(C)$. We present the construction of a differential field extension $\mathcal{L}$ of $F\langle \boldsymbol{a}\rangle$ such that the field of constants of $\mathcal{L}$ is C, the differential Galois group of $\boldsymbol{y}' = A(\boldsymbol{a})\boldsymbol{y}$ over $\mathcal{L}$ is still the full group $G(C)$ and $A(\boldsymbol{a})$ is gauge equivalent over $\mathcal{L}$ to a specialization of $A_G(\boldsymbol{s})$, i.e. to a matrix in normal. In the special case of $G = \mathrm{SL}_3$ we show how one obtains an analogous result for specializations of the coefficients of $A(\boldsymbol{a})$.

Keywords
Differential Galois theory, generic inverse problem, normal forms, gauge equivalence

References

[1] L. GOLDMAN, *Specialization and Picard-Vessiot theory*. Transactions of the American Mathematical Society, 85:327–356, 1957.

[2] L. JUAN AND A. MAGID, Generic rings for Picard-Vessiot extensions and generic differential equations. Journal of Pure and Applied Algebra, 209(3):793–800, 2007.

[3] L. JUAN, Pure Picard-Vessiot extensions with generic properties. Proceedings of the American Mathematical Society, 132(9):2549–2556, 2004.

[4] M. SEISS, Root Parametrized Differential Equations for the Classical Groups. arXiv:1609.05535.

[5] M. SEISS, On the Generic Inverse Problem for the Classical Groups. arXiv:2008.12081.

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *“Computational Differential and Difference Algebra and its Applications”*

Generalized Characteristic Sets and a New Type of Multivariate Difference Dimension Polynomials

Alexander Levin [levin@cua.edu]

Department of Mathematics, The Catholic University of America, Washington, DC 20064, USA

Let K be a difference field of characteristic zero with a basic set of endomorphisms $\sigma = \{\alpha_1, \dots, \alpha_m\}$ (we also called K a σ-field). Suppose that the set σ is represented as the union of p disjoint subsets ($p \geq 1$): $\sigma = \sigma_1 \cup \dots \cup \sigma_p$. Let T denote the free commutative semigroup of all power products of the form $\tau = \alpha_1^{k_1} \dots \alpha_m^{k_m}$ ($k_i \in \mathbb{N}$) and for any such element and for any $i \in \{1, \dots, p\}$, let $\operatorname{ord}_i \tau$ be the sum of all exponents k_ν such that $\alpha_\nu \in \sigma_i$. If $r_1, \dots, r_p, s_1, \dots, s_p \in \mathbb{N}$ and $s_i \leq r_i$ for $i = 1, \dots, p$, let $T(r_1, \dots, r_p; s_1, \dots, s_p) = \{\tau \in T \mid s_i \leq \operatorname{ord}_i \tau \leq r_i \, (1 \leq i \leq p)\}$.
We introduce a new type of reduction of difference polynomials over K that uses the effective orders with respect to the sets σ_i (the corresponding concept generalizes the concept of effective order of an ordinary difference polynomial defined in [1]). We consider characteristic sets associated with such a reduction and use their properties to obtain the following result.

Theorem. Let $L = K\langle \eta_1, \dots, \eta_n \rangle$ be a σ-field extension generated by a set $\eta = \{\eta_1, \dots, \eta_n\}$. Then there exists a polynomial $\phi_{\eta|K}(t_1, \dots, t_p, x_1, \dots, x_p)$ in $2p$ variables with rational coefficients and $r_i^{(0)}, s_i^{(0)}, s_i^{(1)} \in \mathbb{N}$ $(1 \leq i \leq p)$ with $s_i^{(1} < r_i^{(0)} - s_i^{(0)}$ such that
$\phi_{\eta|K}(r_1, \dots, r_p, s_1, \dots, s_p) = \operatorname{tr.deg}_K K(\{\tau\eta_j \mid \tau \in T(r_1, \dots, r_p; s_1, \dots, s_p), 1 \leq j \leq n\})$ for all $(r_1, \dots, r_p, s_1, \dots, s_p) \in \mathbb{N}^{2p}$ with $r_i \geq r_i^{(0)}$, $s_i^{(1)} \leq s_i \leq r_i - s_i^{(0)}$.

We give some properties of the polynomial $\phi_{\eta|K}$ and show that it carries more invariants of the extension L/K (that is, parameters that do not depend on the σ-generators of L over K) than previously known difference dimension polynomials (see [2, Chapter 4] and [3]).

Keywords
Difference field extension, Effective order, Dimension polynomial

References

[1] R. M. Cohn, *Difference Algebra.* Interscience, New York, 1965.
[2] A. Levin, *Difference Algebra.* Springer, New York, 2008.
[3] A. Levin, Reduction with Respect to the Effective Order and a New Type of Dimension Polynomials of Difference Modules. To appear in the *Proceedings of ISSAC 2022.* DOI: https://doi.org/10.1145/3476446.3535497.

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *"Computational Differential and Difference Algebra and its Applications"*

Integrable Cases of the Autonomic Polynomial System

Victor Edneral[1,2] [edneral@theory.sinp.msu.ru]

[1] Skobeltsyn Institute of Nuclear Physics, Lomonosov Moscow State University, Moscow, Russia
[2] Peoples′ Friendship University of Russia, Moscow, Russia

The paper considers the relationship between the local integrability of an autonomous two-dimensional ODE system with polynomial right hand sides and its global integrability. A hypothesis is put forward that for the existence of the first integral of motion in a certain region of the phase space it needs the local integrability in the neighborhoods of all points of this domain.

Using the example of a polynomial case of a plane dynamical system, we wrote out the conditions for local integrability near the stationary points and found the constrains on the parameters under which these conditions are satisfied. In this way we found several cases of integrability. Thus, we propose a heuristic method that allows one to determine the cases of integrability of an autonomous ODE with a polynomial right-hand side in the algorithmic way. For the example we chose the parametrized system of the Lunkevich–Sibirskii type [1]

$$\begin{aligned}\dot{x} &= \quad y + a_1x^2 + a_2xy + a_3y^2,\\ \dot{y} &= -x + b_1x^2 + b_2xy + b_3y^2.\end{aligned}$$

In the same way the degenerated dynamical system has been studied [2].

Keywords
Resonance normal form, Integrability, Computer algebra.

References

[1] V.A. LUNKEVICH; K.S. SIBIRSKII, *Integrals of General Differential System at the Case of Center*. Differential Equation, **18**,# 5 (1982) 786–792 (in Russian).

[2] A.D. BRUNO; V.F. EDNERAL; V.G. ROMANOVSKI, *On new integrals of the Algaba-Gamero-Garcia system.* Proceedings of the CASC 2017, Springer-Verlag series: LNCS **10490** (2017) 40–50.

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *"Computational Differential and Difference Algebra and its Applications"*

Twisted Mahler Discrete Residues

Carlos E. Arreche[1]***, Yi Zhang***[2] [arreche@utdallas.edu]

[1] Department of Mathematical Sciences, The University of Texas at Dallas, Texas, USA
[2] Department of Foundational Mathematics, Xi'an Jiaotong-Liverpool University, Suzhou, CHINA

Continuous residues are fundamental tools in complex analysis, and have compelling applications in combinatorics. In the last decade, a theory of discrete residues and q-discrete residues was proposed by Chen and Singer in [4] for the study of telescoping problems, and it has since found applications in a number of related problems, particularly in the development of algorithms to compute differential Galois groups for (shift and q-dilation) difference equations in [1,2]. We refer to the introduction and references in [3] for more details.

Very recently in [3] we developed a notion of *Mahler discrete residues*, and proved that they comprise a complete obstruction to the *Mahler summability problem* of deciding, for a given integer $p \geq 2$ and $f(x) \in \mathbb{K}(x)$, the field of rational functions in an indeterminate x with coefficients in an algebraically closed field $\mathbb{K}$ of characteristic zero, whether there exists $g(x) \in \mathbb{K}(x)$ such that $f(x) = g(x^p) - g(x)$. This is in analogy with the properties of the discrete residues and q-discrete residues of Chen and Singer in [4], which comprise complete obstructions to the (q-)summability problems of deciding, for a given $f(x) \in \mathbb{K}(x)$, whether $f(x) = g(x+1) - g(x)$ (in the *shift case*) or whether $f(x) = g(qx) - g(x)$ for some $g(x) \in \mathbb{K}(x)$ and $q \in \mathbb{K}$ neither zero nor a root of unity (in the *q-dilation case*). Each of these summability problems is a special case of a more general *telescoping problem*. For σ a $\mathbb{K}$-linear automorphism of $\mathbb{K}(x)$ (for example, the *shift operator* $\sigma : g(x) \mapsto g(x+1)$ or the *q-dilation operator* $\sigma : g(x) \mapsto g(qx)$, for $q \in \mathbb{K}$ as above), one lets δ be a derivation of $\mathbb{K}(x)$ that commutes with σ, that is, such that $\sigma \circ \delta = \delta \circ \sigma$. In the shift case one takes the usual derivation $\delta = \frac{d}{dx}$, and in the q-dilation case one takes the Euler derivation $\delta = x\frac{d}{dx}$. In either case we say $(\mathbb{K}(x), \sigma, \delta)$ is a *$\sigma\delta$-field*, and the corresponding telescoping problem is to decide, for $f(x) \in \mathbb{K}(x)$, whether there exist a *certificate* $g(x) \in \mathbb{K}(x)$ and a linear differential operator $\mathcal{L} \in \mathbb{K}[\delta]$ such that $\mathcal{L}(f) = \sigma(g) - g$. In this case we say $\mathcal{L}$ is a *telescoper* for f. The discrete and q-discrete residues of Chen and Singer in [4] reduce the question of the existence of a telescoper $\mathcal{L} \in \mathbb{K}[\delta]$ to linear algebra over $\mathbb{K}$, all whilst bypassing the potentially expensive computation of a certificate $g \in \mathbb{K}(x)$.

The corresponding summability and telescoping problems in the case of the *Mahler operator* $\sigma : g(x) \mapsto g(x^p)$ for some integer $p \geq 2$ are technically more complicated. First, because σ is only an endomorphism of $\mathbb{K}(x)$ and not an automorphism, it is often (though not always) convenient to replace the usual basefield of rational functions $\mathbb{K}(x)$ with the overfield $\mathbb{K}(x_n)_{n\geq 0}$ where the family of indeterminates x_n are decreed to satisfy $x_n^p = x_{n-1}$ for $n \geq 1$; morally, we think of x_n as x^{1/p^n} for some base indeterminate $x := x_0$. We write, as a matter of notation, $\mathbb{K}(x^{1/p^\infty}) := \mathbb{K}(x_n)_{n\geq 0}$, so that now $\sigma : g(x) \mapsto g(x^p)$ is an automorphism of $\mathbb{K}(x^{1/p^\infty})$. A second technical difficulty is that even this larger field does not admit a derivation δ commuting with σ. This additional technical issue is often (though not always) addressed by introducing a new indeterminate denoted "$\log x$", which is decreed to satisfy the usual properties of the natural logarithm: $\sigma(\log x) = p \log x$ and $\frac{d}{dx}\log x = x^{-1}$, and endowing the field $\mathbb{K}(x^{1/p^\infty})(\log x)$ with the derivation $\delta = (\log x)x\frac{d}{dx}$, which together with the Mahler operator σ makes it into a $\sigma\delta$-field, because we now again have $\sigma \circ \delta = \delta \circ \sigma$.

We study Mahler summability and telescoping problems over $\mathbf{K} := \mathbb{K}(x^{1/p^\infty})((\log x))$ the field of formal Laurent series in the indeterminate $\log x$ with coefficients in $\mathbb{K}(x^{1/p^\infty})$. The basefield of interest $\mathbb{K}(x^{1/p^\infty})(\log x)$ is embedded into $\mathbf{K}$ in the natural way, along with the natural extensions of the Mahler operator σ and the commuting derivation δ, making once again $\mathbf{K}$ into a $\sigma\delta$-field. There is an analogous telescoping problem over this field: given

$$F(x) := \sum_{\lambda \geq N} f_\lambda(x) \log^\lambda x \in \mathbf{K},$$

where $\log^\lambda x := (\log x)^\lambda$ for $\lambda \in \mathbb{Z}$, and each $f_\lambda(x) \in \mathbb{K}(x^{1/p^\infty})$, does there exist $G(x) \in \mathbf{K}$ and $\mathcal{L} \in \mathbb{K}[\delta]$ such that $\mathcal{L}(F) = \sigma(G) - G$? Our main interest in summability and telescoping in the Mahler case over $\mathbf{K}$ is motivated by questions that arise naturally in the computation of (differential) Galois groups associated with Mahler difference equations.

In order to address Mahler summability and telescoping over $\mathbf{K}$, we introduce the notion of (twisted) λ-*Mahler discrete residues* for $\lambda \in \mathbb{Z}$, which will comprise a complete obstruction to the corresponding (twisted) λ-*Mahler summability problem*: given $f_\lambda(x) \in \mathbb{K}(x^{1/p^\infty})$ for some $\lambda \in \mathbb{Z}$, does there exist $g_\lambda(x) \in \mathbb{K}(x^{1/p^\infty})$ such that $f_\lambda(x) = p^\lambda g_\lambda(x^p) - g(x)$? This is directly related to the summability problem for $F = \sum_\lambda f_\lambda \log^\lambda x \in \mathbf{K}$ as above, because a term-by-term computation immediately shows that $F = \sigma(G) - G$ for some $G \in \mathbf{K}$ if and only if, for every $\lambda \in \mathbb{Z}$, $f_\lambda = p^\lambda \sigma(g_\lambda) - g_\lambda$ for some $g_\lambda \in \mathbb{K}(x^{1/p^\infty})$, namely by setting $G = \sum_\lambda g_\lambda \log^\lambda x$. In further analogy with the shift and q-dilation settings, the collection of λ-Mahler discrete residues for $\lambda \in \mathbb{Z}$ reduce the existence of a telescoper $\mathcal{L} \in \mathbb{K}[\delta]$ for $F \in \mathbf{K}$ to linear algebra over $\mathbb{K}$.

Keywords
Mahler difference equations, discrete residues, summability, creative telescoping

References

[1] C.E. Arreche, Computation of the difference-differential Galois group and differential relations among solutions for a second-order linear difference equation. *Communications in Contemporary Mathematics* **19**(6), Article 1650056 (2017).
[2] C.E. Arreche and Y. Zhang, Computing differential Galois groups of second-order linear q-difference equations. *Advances in Applied Mathematics* **132**, Article 102273 (2022).
[3] C.E. Arreche and Y. Zhang, Mahler discrete residues and summability for rational functions. In *Proceedings of the 2022 International Symposium on Symbolic and Algebraic Computation* Villeneuve-d'Ascq, France *(ISSAC '22)* Association for Computing Machinery, New York, NY, In Press, (2022).
[4] S. Chen and M.F. Singer, Residues and telescopers for bivariate rational functions.

Advances in Applied Mathematics **49**(2), 111–133 (2012).

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *"Computational Differential and Difference Algebra and its Applications"*

Reynolds algebras and their free objects by Gröber-Shirshov bases

***Xing Gao*[1], *Li Guo*[2], *Tianjie Zhang*[3]** [liguo@rutgers.edu]

[1] Lanzhou University, Lanzhou, China
[2] Rutgers University, Newark, US
[3] Ningxia University, Yinchuan, China

Reynolds algebras originated from the celebrated work of Reynolds in 1895 on turbulence theory in fluid mechanics. The subject has attracted broad interests in recent years. In this talk we review general background on Reynolds algebras. We then constructs free Reynolds algebras, responding to a problem posed by G. Birkhoff in 1961. The structures of rooted trees and bracketed words, and the method of Gröbner-Shirshov bases are applied.

Keywords
Reynolds operator, Reynolds algebra, Gröbner-Shirshov basis, free object, bracketed word

References

[1] G. BIRKHOFF, Lattices in applied mathematics, II Averaging operators, *Proc. Symp. Pure Math.* **2** 163-184 (1961).

[2] O. REYNOLDS, On the dynamic theory of incompressible viscous fluids and the determination of the criterion, *Phil. Trans. Roy. Soc. A* **136**, 123-164 (1895).

[3] G.-C. ROTA, Reynolds operators, *Proc. Sympos. Appl. Math* **XVI** 70-83 (1964).

[4] T. ZHANG, X. GAO, L. GUO, Reynolds algebras and their free objects from bracketed words and rooted trees. *J. Pure Applied Algebra* **225**, 106766 (2021).

[5] X. GAO, L. GUO, TIANJIE ZHANG, *Construction of free commutative Reynolds algebras by Gröber-Shirshov bases*, preprint, 2022.

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *“Computational Differential and Difference Algebra and its Applications”*

Elimination of unknowns in dynamical systems

Antonio Jiménez-Pastor[1]***, Alexey Ovchinnikov***[2]***, Sonia L. Rueda***[3] [sonialuisa.rueda@upm.es]

[1] LIX, CNRS, École Polytechnique, Institute Polytechnique de Paris, Palaiseau, France
[2] CUNY Queens College and Graduate Center, New York, USA
[3] Dpto. de Matemática Aplicada, Universidad Politécnica de Madrid, Spain

We will discuss elimination of unknowns to simplify systems of difference-differential equations with parameters. For this task we will analyze how different approaches using differential and difference resultants can help in this process.

Existing algorithms for the computation of differential [1] and difference [2] resultants use prolongation and specialization techniques. Prolongation of a given set of n differential (difference) polynomials in $n-1$ differential (difference) variables to obtain a system $\mathcal{S}$ of L polynomials in $L-1$ algebraic variables. Specialization of a Sylvester style coefficient matrix of $\mathcal{S}$ to obtain a multiple of the resultant.

When considering differential-difference (DD) polynomials similar prolongation techniques can be applied, but alternative methods are needed to achieve elimination of the desired variables when applied to models in biology.

Keywords
difference-differential polynomials, resultants

References

[1] S.L. RUEDA, Differential elimination by differential specialization of Sylvester style matrices. Advances in Applied Mathematics, 72, 4-37. *Advances in Applied Mathematics* **72**, 4-37 (2016).

[2] C. M. YUAN, Z. Y. ZHANG, New bounds and an efficient algorithm for sparse difference resultants. In *Journal of Symbolic Computation*, **107**, 279-298 (2021).

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *Computational Differential and Difference Algebra and its Applications*

Algorithmic detection of conserved quantities of finite-difference schemes using difference algebra

Diogo Gomes[1]***, Friedemann Krannich***[1]***, Ricardo de Lima Ribeiro***[1] `[friedemann.krannich@web.de]`

[1] AMCS Program, CEMSE Division, King Abdullah University of Science and Technology, Thuwal, Saudi-Arabia

Many partial differential equations (PDEs) admit integral quantities, that are conserved in time. When approximating a PDE by a finite-difference scheme, the question arises whether related discretized quantities remain conserved by the scheme. Such information can be crucial to estimate whether a scheme approximates a PDE accurately and to determine its stability.

Computations for determining conservation can get rather tedious. Hence, automating them in computer algebra systems is desirable.

Conserved quantities correspond to conservation laws, admitted by the PDE. A conservation law [1] is an equation of the form

$$D_t\Phi[u] + D_x\Psi[u] = 0$$

holding for all solutions u of the considered PDE, that induces the conserved quantity $\int \Phi[u]\, dx$ as

$$\frac{d}{dt}\int \Phi[u]\, dx = \int D_t\Phi[u]\, dx = -\int D_x\Psi[u]\, dx = 0$$

assuming periodic boundary conditions in x.

An analog formulation describes conservation laws for schemes of PDEs, where the derivatives are replaced by differences. The key for the construction of schemes, that admit certain conservation laws from the continuous PDE, is the use of the discrete Euler operator [1] (also called discrete variational derivative). Kupershmidt discovered, that an equation is a discrete conservation law if and only if it belongs to the kernel of the discrete Euler operator [6]. Hence, standard approaches for constructing schemes with conservation are either discretizing the continuous conservation law or finding multipliers for the scheme, such that the result is in the kernel of the discrete Euler operator [1].

This strategy was, for example, recently used by Dorodnitsyn et al. to develop a scheme for the shallow water equation, that preserves energy [2]. Cheviakov et al. used this idea to find schemes for the linear and nonlinear wave equation, that admit several discrete analogs of continous conservation laws [1].

Hereman et al. [5] proposed an algorithm to compute conserved densities for semi-discretized schemes for PDEs with first-order time derivative. Their algorithm uses the scaling symmetries of the scheme to construct conserved quantities and calculates their coefficients using the discrete Euler operator.

In this talk, we describe an approach, that uses difference algebra to check, if a quantity is conserved in time under a finite-difference scheme. Our approach differs from the ideas described above, as we do not try to construct discrete Φ and Ψ, using the scheme, but we check if a given discrete Φ is conserved in time under a given scheme.

Gerdt showed [3], that a quantity is conserved, if its discrete time derivative belongs to the difference ideal generated by the scheme. However, some quantities may add to a constant (e.g. telescopic sums) and thus be trivially preserved without belonging to the difference ideal. Moreover, Gerdt's algorithm may not terminate, as the Gröbner basis for the difference ideal may not be finite. We overcome these issues by combining the discrete partial variational derivative with a polynomial ideal instead of a difference ideal with finite Gröbner basis. We have implemented this algorithm as part of a package in MATHEMATICA [7]. We show that our code finds conserved quantities and proper schemes for the time-implicit and time-explicit discretization of the Burgers equation and a system of PDEs arising in the study of mean-field games.

This talk is based on the preprint [4].

Keywords

Symbolic computations, Finite-difference schemes, Discrete variational derivative, Discrete partial variational derivative, Conserved quantities, Difference algebra

References

[1] A. CHEVIAKOV, V. DORODNITSYN, E. KAPTSOV, Invariant conservation law-preserving discretizations of linear and nonlinear wave equations. *Journal of Mathematical Physics* **61**(8), 081504 (2020).

[2] V. DORODNITSYN, E. KAPTSOV, Discrete shallow water equations preserving symmetries and conservation laws. *Journal of Mathematical Physics* **62**(8), 083508 (2021).

[3] V. GERDT, Consistency Analysis of Finite Difference Approximations to PDE Systems. In *Mathematical Modeling and Computational Science*, G. Adam, J. Buša, M. Hnatič, 28–42, Springer, Berlin Heidelberg (2012).

[4] D. GOMES, F. KRANNICH, R. RIBEIRO, Algorithmic detection of conserved quantities of finite-difference schemes for partial differential equations. *Preprint* (2022).

[5] W. HEREMAN, J. SANDERS, J. SAYERS, J.P. WANG, Symbolic Computation of Polynomial Conserved Densities, Generalized Symmetries, and Recursion Operators for Nonlinear Differential-Difference Equations. *CRM Proceedings and Lecture Notes* **39**, 133–148 (2004).

[6] A. KUPERSHMIDT, Discrete Lax equations and differential-difference calculus. *Astérisque* **123** (1985).

[7] WOLFRAM RESEARCH, INC., Mathematica, Version 13.0.0.
https://www.wolfram.com/mathematica, Champaign, IL (2021).

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *"Computational Differential and Difference Algebra and its Applications"*

Holonomic modules and 1-generation in the Jacobian Conjecture

V. V. Bavula [v.bavula@sheffield.ac.uk]

School of Mathematics and Statistics, University of Sheffield, UK

The Jacobian Conjecture, the Conjecture of Dixmier and the Poisson Conjecture are questions about whether certain algebra/Poisson endomorphisms are epimorphisms. We show that the Jacobian Conjecture, the Conjecture of Dixmier and the Poisson Conjecture are questions about holonomic modules for the Weyl algebra A_n. This fact allows us to measure the 'size' of the images of the maps. Using this approach we show that the images of the Jacobian maps, endomorphisms of the Weyl algebra A_n and the Poisson endomorphisms are large in the sense that further strengthening of the results on largeness would be either to prove the conjectures or produce counter examples. A short direct algebraic proof (without reduction to prime characteristic) is given of equivalence of the Jacobian and the Poisson Conjectures (this gives a new short proof of equivalence of the Jacobian, Poisson and Dixmier Conjectures).

Keywords
The Jacobian Conjecture, the Conjecture of Dixmier, the Poisson Conjecture

References

[1] V. V. BAVULA, Holonomic modules and 1-generation in the Jacobian Conjecture. (2021) *arXiv:2112.03177*.

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *"Computational Differential and Difference Algebra and its Applications"*

Computing the exceptional parameter set for a family of linear differential equations

Ruyong Feng[1], ***Michael Wibmer***[2] [wibmer@math.tugraz.at]

[1] Key Lab of Mathematics Mechanization, Chinese Academy of Sciences, Beijing, China
[2] Institute of Analysis and Number Theory, Graz University of Technology, Graz, Austria

Based on a study of torsion points on abelian varieties, Masser and Zannier [1] recently showed that the set of values of t such that an algebraic function $f_t(x)$, depending on a parameter t, can be integrated (with respect to x) in elementary terms, is "small", in fact, often finite, if $f_t(x)$ cannot be integrated in elementary terms generically (i.e., when t is considered to be transcendental). As integration can be seen as solving a very particular differential equation, it is natural to wonder about generalizations to linear differential equations. More precisely:

Let k be an algebraically closed field of characteristic zero and let B be a finitely generated k algebra that is an integral domain. Furthermore, let $f \in B[x]$ be a monic polynomial. We think of a linear differential equation $y' = Ay$, with $A \in {B[x]_f}^{n\times n}$ as a family of linear differential equations parametrized by the algebraic variety $X = \operatorname{Spec}(B)$: Applying $c \in X(k) = \operatorname{Hom}_k(B, k)$ to the coefficients of the entries of A, one obtains a specialized linear differential equation $y' = A^c y$ over $k(x)$.

If $y' = Ay$ does not have a basis of Liouvillian solutions, it is natural to expect that the *exceptional set* of all $c \in X(k)$ such that $y' = A^c y$ has a basis of Liouvillian solutions is "small". However, in this situation, we typically cannot expect a finiteness result. For example, if $B = k[\alpha]$, $f = x$ and

$$A = \begin{pmatrix} 0 & 1 \\ (\frac{\alpha}{x})^2 - 1 & -\frac{1}{x} \end{pmatrix} \in B[x]_f = k[\alpha, x]_x$$

is the companion matrix of Bessel's differential equation $y'' + \frac{1}{x}y' + (1 - (\frac{\alpha}{x})^2)y = 0$, then the exceptional set is $\{m + \frac{1}{2} |\, m \in \mathbb{Z}\}$.

Due to the lack of finiteness of the exceptional set, a notion encapsulating the "smallness" of the exceptional set is needed. Generalizing a result of Hrushovski from [2], we show that the exceptional set is indeed "small" in an appropriate sense and we describe the various sources that yield exceptional points of the parameter space.

Indeed, we establish a general specialization theorem for the differential Galois group of a linear differential equation, that can be used to transfer results in inverse differential Galois

theory over the rational function field from one single field of constants to an arbitrary field of constants. Our prime illustration of this principle is the completion of our program to establish Matzat's conjecture ([3,4,5,6]): The absolute differential Galois group of a one-variable function field over k, equipped with a non-trivial k-derivation, is the free proalgebraic group on a set of cardinality $|k|$.

Keywords
Specializations of differential Galois groups, families of linear differential equations, Matzat's conjecture

References

[1] D. MASSER; U. ZANNIER, Torsion points, Pell's equation, and integration in elementary terms. *Acta Math.* **225**(2), 227–313, (2020).
[2] E. HRUSHOVSKI, Computing the Galois group of a linear differential equation. Differential Galois theory (Będlewo, 2001), 97–138, Banach Center Publ., 58, Polish Acad. Sci. Inst. Math., Warsaw, 2002.
[3] M. WIBMER, Free proalgebraic groups. *Épijournal Géom. Algébrique* **4**, Art. 1, 36 pp. (2020)
[4] A. BACHMAYR; D. HARBATER; J. HARTMANN; M. WIBMER, Free differential Galois groups. *Trans. Amer. Math. Soc.* **374**(6), 4293–4308, (2021).
[5] A. BACHMAYR; D. HARBATER; J. HARTMANN; M. WIBMER, The differential Galois group of the rational function field. *Adv. Math.* **381**, Paper No. 107605, 27 pp. (2021).
[6] M. WIBMER, Subgroups of free proalgebraic groups and Matzat's conjecture for function fields, to appear in *Israel Journal of Mathematics*, ArXiv:2102.02553.

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *Computer Algebra in Education*

Computer Algebra Systems – powerful tools for creating teaching-learning resources in undergraduate mathematics

Elena Varbanova[1] [elvar@tu-sofia.com]

[1] Faculty of Applied Mathematics and Informatics, Technical University of Sofia, Bulgaria

Ideas, approaches and tools for enhancement of undergraduate engineering mathematics are considered. A long lasting experiment with constant improvements in development and implementation of basic elements of holistic education - through development of the student's full potential, has proved a synergy effect of these activities. Some of them are represented. Computer Algebra Systems (CASs) are considered as a means to improve the overall effect of the quality of teaching-learning resources (TLR) on the student's learning path (trajectory). This quality is looked to with the hope of creating effective learning.

Two of the leading sentences for us are: "Knowledge can help you move from a point A to a point B, imagination can bring you from A to any other point" (A. Einstein) and "An individual's incorrect thoughts are due to insufficient development of his/her ability to distinguish" (Paramahansa Yogananda).

What we were trying to do is keeping the focus on the student/learner and the learning. We started with using different colors for different content and learning outcomes, e.g. new terms and definitions are highlighted in one color, important statements and sentences in another ([1, 2, 3, 4]) . In addition, different symbols enable a clear presentation of the content and make TLR easy to read/follow, e.g. a special symbol for pointing out that one often overlooks, ignores or wrongly understands or interprets.

Tips and rules are used to make it easier to work through the examples and exercises; structuring points and orientation aids are provided; the summaries are highlighted in color; important formulas and results are marked; model examples are appropriately placed in the text. Thoroughly calculated examples, tasks with solutions, illustrations and visualizations are included.

The next figures (figure 1 and figure 2) show an application of CAS *Derive* :

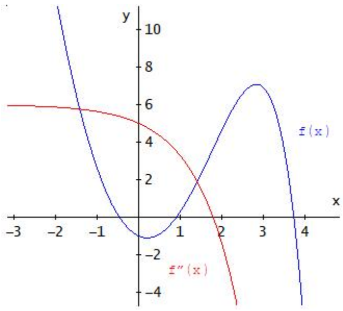


Figure 1: Graphical illustration of geometrical prototype of a sufficient condition for the convergence of an iterative method for solving nonlinear equations

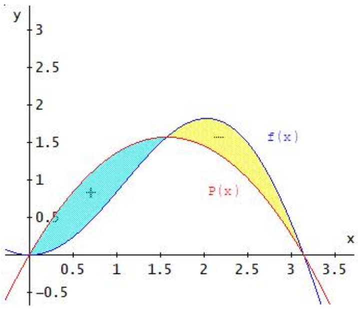


Figure 2: Graphical illustration of geometrical prototype of a rule for numerical integration and the error of the approximation value

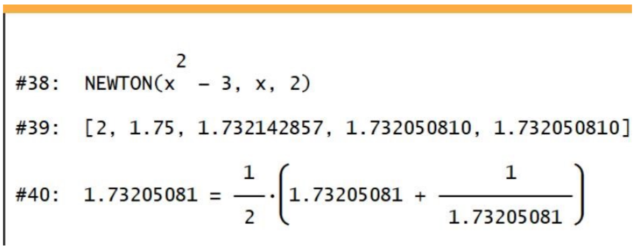
The impact of colors on correct calculation of partial derivatives by students are illustrated by the next two equalities. And the correct rearrangement of terms in an ordinary differential equation is illustrated by the third one.

$$\Big(x^2\, y \sin x\Big)_x = \Big|\, y \text{ is treated as a constant} \,\Big| = y\, \underbrace{(2x\, \sin x + x^2\, \cos x)}_{\text{Product rule}}$$

$$\Big(\tan(x-y)\Big)_y = \underbrace{\frac{1}{\cos^2(x-y)}\,(x-y)_y}_{\text{Chain rule}} = \frac{1}{\cos^2(x-y)}\,(0-1) = -\frac{1}{\cos^2(x-y)}$$

$$\frac{\cos x}{1+y^2}\,\frac{dy}{dx} = \sin(x) \Rightarrow \frac{dy}{1+y^2} = \frac{\sin(x)}{\cos(x)}\,dx \Rightarrow \int \frac{1}{1+y^2}\,dy = \int \frac{\sin(x)}{\cos(x)}\,dx$$

CASs can be used for creating non-trivial questions to check the deepness of students' knowledge and to help them master the competence “reflection”. For instance, we ask them to “read”/explain the lines #38 and #39 of figure 3. The student has to develop the ability for controlling the results (critical thinking), i.e. to built up the competence "reflection". If so,



```
               2
#38:  NEWTON(x  - 3, x, 2)

#39:  [2, 1.75, 1.732142857, 1.732050810, 1.732050810]

                    1  ⎛                    1        ⎞
#40:  1.73205081 = ———·⎜1.73205081 + ——————————————⎟
                    2  ⎝               1.73205081  ⎠
```

Figure 3: Newton's method with *Derive*

he/she can guess the relationship between the terms of the sequence in #39 and #40 of figure 3. For example, it has to be clear to him/her that there exists the relationship between the third and fourth number in #39 of figure 3.

And it has to be related to the third iteration obtained by Newton's method (abstract thinking):

$$x_{n+1} = \frac{1}{2}\left(x_n + \frac{3}{x_n}\right), n = 0, 1, 2.$$

In general, one needs to "read" symbolic, numerical, and graphical results and interpret them correctly. And to know that the components in the chain Knowledge-Skills-Control (Reflection) are interrelated. ("One can see as much as one knows.")

About Microlearning ([5]). Microlearning is a skill-based approach to learning that delivers information in small, highly focused chunks. A microlearning module (= a learning unit) is "as long as necessary and as short as possible". Learners tend to engage with microlearning more often, which increases learning retention. Microlearning is a strategy where independent learning units work for a single purpose and are part of the total learning picture.

Illustration of microlearning module and step-by-step (structured) approach to the solution. Solve the following ordinary differential equation of order one : $y' - y\tan(x) = \exp(\sin(x))$.
Solution.

- Step 0. Recognition of the type of the equation
- Step 1. Extraction of necessary information
- Step 2. Writing the formula for the general solution of a linear equation
- Step 3. Determination of the integrating factor
- Step 4. Replacement of the corresponding functions into the formula in Step 2
- Step 5. Solution of the integral in the right-hand side
- Step 6. Final answer (using Step 4 and Step 5): the general solution.

To communicate and collaborate with peers and engage on educational tasks students are provided questions for self-preparation; the opportunities of CASs are used for setting the questions up. The represented ideas and approaches for creating TLR can be used for blended or hybrid learning considered as a learning approach that combines traditional/conventional teaching-learning-assessment (TLA) process and remote learning activities. Purposeful and appropriate TLR could be effective in bridging the gap among remote and conventional learning and so to contribute to improve the hybrid learning. During the TLA process students develop learning abilities and habits, as well as educational values that are helpful for the real life and, above all, for their work. "Future of Work Is Nothing Without Consideration For The Future of Learning" ([6]). Future of learning solutions require the components of the triad Teaching-Learning-Assessment to become interdependent, not stand alone.

Keywords
Undergraduate mathematics, teaching-learning-resources, CASs, micro-learning.

References

[1] T. Arens, F. Hettlich, Ch. Karpfinger, U. Kockelhorn, K. Lichtenegger, H. Stacbel. *Mathematik*, Spectrum Akademischer Verlag, Heidelberg, 2008.

[2] E. Varbanova, *Calculus*1*, Lectures*, TU-Sofia, Sofia, 2009.

[3] E. Varbanova, *Calculus*1*, Exercises and laboratory classes*, TU-Sofia, Sofia, 2011.

[4] T. Westermann, *Mathematik für Ingenieure*, Springer Verlag (ebook), 2015

[5] *Microlearning : A must in 2022* (ispringsolutions.com).

[6] `https://modernlearners.com/future-of-learning/`

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *Computer Algebra in Education*

Using CAS in the classroom: personal thoughts (Part II)

Michel Beaudin[1] [michel.beaudin@etsmtl.ca]

[1] Service des enseignements généraux, École de technologie supérieure, Montréal (QC), Canada

In this presentation, we will continue our reflection started at ACA2021 about the use of computer algebra in the classroom. Trying to find examples of how CAS technology can be easily used to teach subjects where only pencil and paper techniques would discourage the user. Examples that should appear in textbooks but, unfortunately, not so often. At the last ACA conference (virtual ACA2021), we focused on how computer algebra could help to understand how third degree polynomial roots should be simplified. We wrote that future ACA conferences could cover more examples: trying to update some integration tables in relation with the Rubi system and trying to use computer algebra to teach some parts of complex analysis.

This year, we chose complex analysis because it doesn't seem to fit with computer algebra. But many concepts in analysis can be introduced and/or illustrated by CAS. We will look at some examples:

- how the user can visualize the complex roots of a polynomial using 2D and 3D plots;
- how Laurent series, residue integration techniques and numerical line integrals can be combined to verify some answers;
- how to use a built-in Rieman Zeta function to observe some non trivial zeros of $\zeta(s)$.

Nspire CX CAS and Maple software will be used.

Applications of Computer Algebra – ACA 2022
August 15-19, 2022
Session on *Computer Algebra in Education*

Simplified models of planetary orbits, virtual space mandalas and beyond

Thierry Dana-Picard[1] [ndp@jct.ac.il]

[1] Department of Mathematics, Jerusalem College of Technology, Jerusalem, Israel

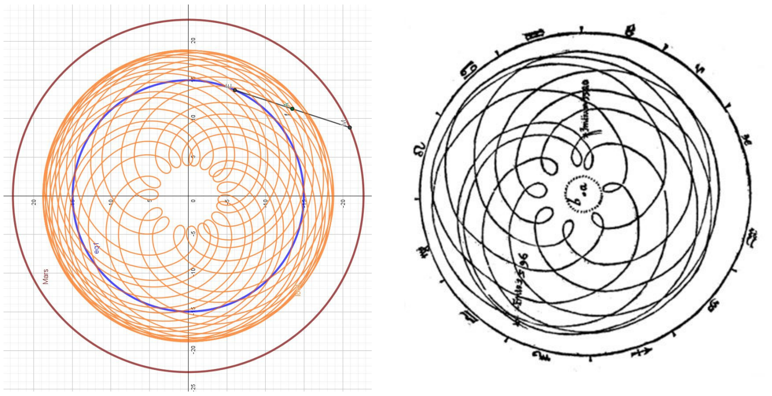
Generally, in books such as [1] and online catalogues of plane curves, such as [2,3], the curves are presented individually. In many cases, strong connections can be revealed. Studying isoptic curves in [4], we showed a strong connection between conic sections and toric sections. The toric section are quartics, sometimes called also spiric curves. An important property is that they are the intersection of self-intersecting tori with a plane, which is not frequent in the literature. Internal connections between these curves have been shown in [5], as the Hessian of a spiric is also a spiric. This enabled to determine the points of inflexion of these curves.

Networking between a Computer Algebra System (CAS) and a Dynamic Geometry System (DGS), as in [6], we study some plane curves given by parametric presentations. The ubiquitous articles in newspapers about spacecrafts, in particular about the triple launch towards Mars 2 years ago, incited students to ask questions about their trajectories and , in general, about modeling planetary orbits. Using simple models of circular orbits centered at the Sun, with constant velocity, we defined the loci of some virtual points (we mean points which do not have a strong physical meaning, but can be studied with mathematical methods). Figure 1(a) has been obtained with software, using GeoGebra's **Locus** command and an animation. Figure 1(b) is Kepler hand-drawing of Mars's orbit viewed from the Earth [7]. This yields a great number of curves, which artists call mandalas. We obtain also generalizations of Lissajous curves. Moreover, the above mentioned catalogues describe families of curves called epitrochoids, hypotrochoids, etc. Exploration with software reveals a uniforming framework for these families.

The needed orbital data is obtained from dedicated websites. The students discover that most of the data is not made of integer numbers, and that every website makes its own decisions regarding the decimal approximations. The usage of a slider bar enables to explore the influence of the precision on the obtained mandalas. At this stage, mostly curves given by parametrizations of the form

$$\begin{cases} x(t) = \cos t + r\cos(\frac{t}{h}) \\ y(t) = \sin t + r\sin(\frac{t}{h}) \end{cases}$$

where r encodes the ratio of orbital radii and h the ratio of orbital velocity, taking here the



(a) The midpoint of Mars and the Earth (b) Mars viewed from the Earth, by Kepler

Figure 1: Two space mandalas

Earth as the first planet. Its distance to the Sun is equal to 1 AU (astronomical unit) and its orbital period is 1 year.

This is where a double slider is useful.

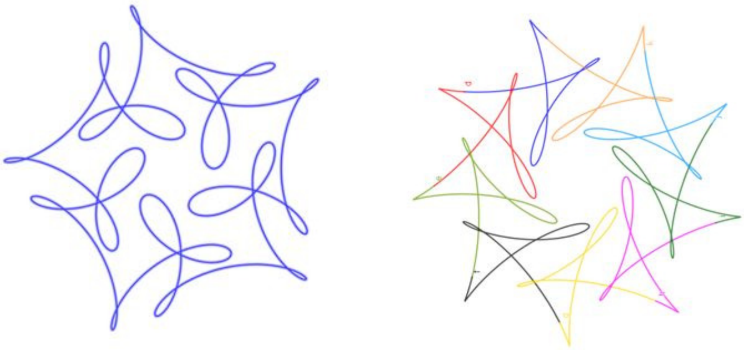
As a generalization, we explore a model with an additional 3^{rd} planet. In this talk, we prefer to show more abstract situations, where the hypothetic 3^{rd} object runs in reverse direction, which is encoded in a parametrization of the form

$$\begin{cases} x(t) = \cos t + b\cos(\omega_1 t) + c\sin(\omega_2 t) \\ y(t) = \sin t + b\sin(\omega_1 t) + c\cos(\omega_2 t) \end{cases}$$

Once again, the first coefficient is equal to 1 as the distance from Earth to the Sun is defined as 1 astronomical unit (AU). For a similar reason, the angular velocity of the Earth is put as 1 (orbital period equal to 1 year). Changing the parameters reveals curves with symmetries of non trivial order (we mean of order 7, 9 , 11, etc.), which are generally not constructed with simple tools. Two examples are on display in Figure 2 .

The symmetries can be enhanced by two means: visually by playing on the plotting intervals and changing the colors, with automated methods by plotting a "basic part" of the curve, then using the automated commands for rotations, algebraically using substitution and trigonometric identities.

Finally, we wish to recall that STEM Education is well-known and documented. During the past decade, new developments occurred and an A has been added, A for Arts, defining STEAM Education [8]. The proposed activities, dominated by M, S and T have a nice A aspect with the space mandalas. that the kind of activities that we propose here is typical of STEAM Education. We have here a mathematical topic with strong connections with the real world and the cultural background of the students (here the daily newspapers), Physics (true, we used a very simplified model) and artistic creation. Technology is the medium which enables to build these connections.



(a) Rotational symmetry of order 5

(b) Rotational symmetry of order 9

Figure 2: Two generalizations of mandalas

Keywords
Automated exploration, parametric curves, mandalas, visual arts, STEM Education

References

[1] R.J. Walker. *Algebraic Curves*, NY: Springer, 1950.
[2] R. Ferréol. Mathcurve, retrieved 2022.
[3] MacTutor Famous Curves Index, retrieved 2022.
[4] Th. Dana-Picard, G. Mann and N. Zehavi. *From conic intersections to toric intersections: the case of the isoptic curves of an ellipse*, The Montana Mathematical Enthusiast 9 (1), 59–76 (2011).
[5] Th. Dana-Picard Inflexion of spirics: a tale of two tori, *ACA 2021*.
[6] Th. Dana-Picard and Z. Kovács: Networking of technologies: a dialog between CAS and DGS, *The electronic Journal of Mathematics and Technology* (eJMT) 15 (1), 17 pages (2021)
[7] Kepler, J. *Astronomia Nova*, 1609.
[8] Aguilera, D. and Ortiz-Revilla, J. (2021). STEM vs. STEAM Education and Student Creativity: A Systematic Literature Review, Education Sciences 11, 331. https://doi.org/10.3390/educsci1107033

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *Computer Algebra in Education*

Comprehensive solutions to problems in Maple, using the parametric option.

D. J. Jeffrey[1] [djeffrey@uwo.ca]

[1] Mathematics Department, The University of Western Ontario, London, Ontario, Canada

It is very common for mathematical problems and mathematical tables to contain parameters. For example, every calculus book contains a table of integrals with entries such as

$$\int x^n \, dx = \frac{x^{n+1}}{n+1}\ , \text{ and } \int \cos(ax)\, dx = \frac{\sin(ax)}{a}\ .$$

Few books bother to write $a \neq 0$, and it is even less likely that anyone of them adds the comment that $a = 0$ has the integral x. If a user asks Maple for the solution of $ax = a$, should Maple reply $x = 1$, or $x = 1, a \neq 0$ or something else? When a problem with parameters has different solutions depending upon the value actually taken by a parameter, then a list of all possibilities is called a comprehensive solution. Early computer algebra systems did not attempt to return comprehensive solutions. Recently, however, Maple has been extending the range of problems for which it can return comprehensive solutions. A user can usually obtain these solutions by specifying the option 'parametric'. In this talk a number of examples of where the option is available will be presented as well as on-going projects that will add the option to new problems.

Keywords
Comprehensive solutions, parametric option, Maple.

References
[1] R. M. CORLESS, D. J. JEFFREY, D. R. STOUTEMYER, Integrals of functions containing parameters, *The Mathematical Gazette*. **104**, 412–426, 2020, doi:10.1017/mag.2020.96

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey | August 15-19, 2022
Session on *Computer Algebra in Education*

Multivalued functions and cubic equations

V. M. Quance[1], ***M. R. Vancea***[1], ***D. J. Jeffrey***[1] [{vquance,mvancea}@uwo.ca]

[1] Mathematics Department, The University of Western Ontario, London, Ontario, Canada

This talk combines a discussion of multivalued functions in computer algebra with the solution of cubic equations. The first solutions to cubic equations were discovered 500 years ago [1], but the discussion of the solutions takes on new dimensions in the age of computer algebra systems. The early solutions of the cubic famously brought the first sight of imaginary numbers to mathematics; they caused “mental agonies" for poor old Cardano. In the modern world, Maple assumes every quantity is complex by default, and this can result in surprises for its users. We shall explain why some sources say the solution of $x^3 + 3px - 2q = 0$ is [2]

$$\left(q + \sqrt{p^3 + q^2}\right)^{1/3} + \left(q - \sqrt{p^3 + q^2}\right)^{1/3} ,$$

but Maple says it is

$$\left(q + \sqrt{p^3 + q^2}\right)^{1/3} - \frac{p}{\left(q + \sqrt{p^3 + q^2}\right)^{1/3}} .$$

We shall also explain why Maple has 2 cube-root functions: $z^{1/3}$ and `surd(z,3)`. We give further consideration to different ways to get solutions of cubics.

Keywords
Multivalued function, Cube root, Inverse function, Cubic equation.

References

[1] GIROLAMO CARDANO, *Ars Magna 1545.* Translated by T.R. Witmer as ‘The great art or Rules of Algebra’, MIT Press, 1968.

[2] M. ABRAMOWITZ AND I. A. STEGUN, *Handbook of Mathematical Functions.* Dover, New York, 1965.

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *"Computer Algebra Modeling in Science and Engineering"*

Designing Physics Problems with *Mathematica*. Example I

Haiduke Sarafian[1] [has2@psu.edu]

[1] The Penssylvania State Uninversity, York, PA, USA

We envision utilizing the versatility of a Computer Algebra System, specifically *Mathematica* to explore designing physics problems. As a focused project we consider for instance a thermo-mechanical-physics problem showing its developmental from the ground up. In accordance with the objectives of this investigation first by applying the fundamentals of physics principles we solve the problem symbolically. Applying the solution we investigate the sensitivities of the quantities of interest for various scenarios generating feasible numeric parameters. Although a physics problem is investigated, the proposed methodology may as well be applied to other scientific fields. The codes needed for this particular project are included enabling the interested reader to duplicate the results, extend and modify them as needed to exploring various extended scenarios.

Keywords
Thermo-Mechanical Physics, Designing Physics Problems, Computer Algebra System, *Mathematica*

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *"Computer Algebra Modeling in Science and Engineering"*

Designing Physics Problems with *Mathematica*. Example II

Haiduke Sarafian[1] [has2@psu.edu]

[1] The Penssylvania State Uninversity, York, PA, USA

Customarily in the physics of sound, static-acoustic-related topics are addressed. For instance, the change in the sound level vs discrete change in the distance. In dynamic cases, e.g. the Doppler shit although the relative motion of the components i.e. the source and the sensor are essential the movements are limited to uniform motions. In this investigating report, scenarios are considered departing these limitations. In the former time-dependent sound level and the latter nonuniform motions are analyzed. Aside from light long-hand mathematical formulations, the majority of the analysis is carried out utilizing a Computer Algebra System (CAS) specifically *Mathematica*. The analysis and the format of the development are crafted flexibly conducive opportunities for furthering quests for the "what if" scenarios.

Keywords
Physics of Sound, Time-dependent Sound Level, Designing Physics Problems, Computer Algebra System, *Mathematica*

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *"Computer algebra modeling in science and engineering"*

Photoelastic and numerical stress analysis of a pin on a plan contact subjected to a normal and a tangential load

Mustapha Beldi, Ali Bilek, and Said Djebali [ali.bilek@ummto.dz]

L.M.S.E. Laboratory, Mechanical Engineering Department, UMMTO University, 15000 Tizi-Ouzou, Algeria

Theoretical studies of contact stresses can be in some cases very complex. Several methods, experimental as well as numerical, have then be used to analyze these types of problems. In this paper two methods have been used: the photoelasticity method and the finite element method. Stresses were determined in the neighborhood of the contact zone for a plan subjected to a normal load and a tangential load via a pin of rectangular cross section. The purpose here is to study the effect of applying simultaneously a normal and a tangential load on the stress field developed in the plan. In the finite element solution, the pin made of aluminum was considered to be rigid relatively to the plan which is made of a birefringent material necessary to analyze optically the model stresses. The photoelastic fringes obtained on the analyzer of a polariscope allowed us to obtain stress values on the plan, particularly in the neighborhood of the contact zone, in order to compare them with the numerical results. Comparisons were also made between experimental and simulated isochromatic and isoclinic fringes. Relatively good agreements have been observed. Problems with more complicated geometries can therefore be studied numerically. Good care should be taken though when dealing with the limit conditions to achieve better simulation.

Keywords
Photoelasticity, Birefringent, Contact stress, Simulation

References

[1] R. L. Burguete; E. A. Patterson, A photoelastic study of contact between a cylinder and a half-space. *Experimental Mechanics* **V.37**(3), 314–324 (1997).
[2] A. Mihailidis; V. Bakolas; N. Drivakovs, Subsurface stress field of a dry line Contact. *Wear* **V. 249**(I.7), 546–556 (2001).
[3] A. Bilek; J. C. Dupre; A. Ouibrahim; F. Bremand, 3D Photoelasticity and numerical analysis of a cylinder/half-space contact problem. *Computer Methods and Experimental Measurements for Surface Effects and Contact Mechanics* **Vol 49**(VII), 173–182 (2000).
[4] B. Mijovic; M. Dzoclo, Numerical Contact of a Hertz Contact Between two Elastic Solids. *Engineering Modeling* **V.13**(3-4), 111–117 (2000).
[5] A. Bilek; F. Djeddi, Photoelastic and numerical stress analysis of a 2D contact problem

and 3D numerical solution for the case of a rigid body on a deformable one. *WIT Transaction on Modeling and Simulation* **Vol 51**( ), 177–187 (2011).
[6] J. W. DALLY; F. W. RILEY, *Experimental stress analysis*. McGraw-Hill, Inc, City, 1991.

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *"Computer algebra modeling in science and engineering"*

Numerical and experimental analysis of stress fields in mechanical contacts between solids (rigid/deformable and deformable/deformable)

Mustapha Beldi, Ali Bilek, and Said Djebali [ali.bilek@ummto.dz]

L.M.S.E. Laboratory, Mechanical Engineering Department, UMMTO University, 15000 Tizi-Ouzou, Algeria

This paper deals with contact problems between solids. This type of problem can be encountered in mechanical systems where contact between moving components can give rise to high stresses, particularly in the neighborhood of contact zones. The analyzed model consists of a birefringent epoxy disk under diametric compression between two plates, one made of a birefringent epoxy and the other one made of steel. The model allows therefore analyzing on a polariscope, with plan polarized light and circularly polarized light, both types of contact (rigid/deformable and deformable/deformable). A numerical solution is used to determine stresses in the whole model, particularly in the neighborhood of the contact zones. Simulated isochromatic fringes and isoclinic fringes are compared to the experimental ones obtained on the analyzer of a polariscope. Relatively good agreements are achieved between the experimental solution and the finite element solution; by zooming on the contact zones one can see that photoelastic fringes show clearly the areas of maximum shear stresses and their relative positions in the neighborhood of the contact zones. Comparison is also made with theoretical results obtained by Hertz theory of contact.

Keywords
Contact stress, Birefringent, Isochromatic, isoclinic, Simulation

References

[1] A. BILEK; J. C. DUPRE; A. OUIBRAHIM; F. BREMAND, 3D Photoelasticity and numerical analysis of a cylinder/half-space contact problem. *Computer Methods and Experimental Measurements for Surface Effects and Contact Mechanics* **Vol 49**(VII), 173–182 (2000).
[2] R. S.ABODOL; A. M. GOUDARZI; R. A. ALASHTI, Finite Element Analysis of Elastic-Plasti Contact Mechanic Considering the Effect of Contact Geometry and Material Propertie. *Journal of Surface Engineered Materials and Advanced Technology* **V.1**(3), 125–129 (2011).
[3] B. MIJOVICAND; M. DZOCLO, Numerical contact of a Hertz contact between two elastic solids. *Engineering Modeling* **17**(3-4), 111–117 (2000).
[4] A. BILEK; F. DJEDDI, Photoelastic and numerical stress analysis of a 2D contact problem

and 3D numerical solution for the case of a rigid body on a deformable one. *WIT Transaction on Modeling and Simulation* **Vol 51**( ), 177–187 (2011).

[5] K. RAMESH; T. KASIMAYAN; S. B. NEETHI;, Digital photoelasticity - A comprehensive review. *The Journal of Strain Analysis for Engineering Design* **Vol. 46**(4), 245–266 (2011).

[6] J. W. DALLY; F. W. RILEY, *Experimental stress analysis*. McGraw-Hill, Inc, City, 1991.

[7] K. L. JOHNSON, *Contact mechanics*. Cambridge University press, 1985.

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *“Computer algebra modeling in science and engineering”*

Discrete models of epidemic spread in a heterogeneous population

Marcin Choiński[1] ***, Mariusz Bodzioch***[2]***, Urszula Foryś*** [3] [marcin_choinski@sggw.edu.pl]

[1] Warsaw University of Life Sciences, Faculty of Applied Informatics and Mathematics, Warsaw, Poland
[2] University of Warmia and Mazury in Olsztyn, Faculty of Mathematics and Computer Science, Olsztyn, Poland
[3] Institute of Applied Mathematics and Mechanics, Faculty of Mathematics, Informatics and Mechanics, University of Warsaw, Poland, Warsaw, Poland

We will present discrete models of epidemic spread in a population in which we consider two groups of people: with a low risk of an infection and with a high one. These models are built with the use of the explicit Euler method and the non-standard discretization. We will focus on stability analysis of stationary states appearing in the systems. In the case of the non-standard discretization we will also consider a simplified version of the model in which we assume that there is no transmission of the infection from the group of the low risk of the infection to the group of the high one. The theoretical results will be complemented with numerical simulations.

Keywords
epidemiology, the explicit Euler method, non-standard discretization

References

[1] M. CHOIŃSKI, M. BODZIOCH, U. FORYŚ, A non-standard discretized SIS model of epidemics. *Mathematical Biosciences and Engineering* **19**(1), 115–133 (2022).
[1] M. CHOIŃSKI, M. BODZIOCH, U. FORYŚ, Simple discrete SIS criss-cross model of tuberculosis in heterogeneous population of homeless and non-homeless people, *Mathematica Applicanda*, **47**(1), 103–115, (2019).

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *"Computer Algebra Modeling in Science and Engineering"*

Fitting Sparse Reduced Data

Ryszard Kozera[1] [ryszard_kozera@sggw.edu.pl]

[1] Institute of Information Technology, Warsaw University of Life Sciences – SGGW, Warsaw, Poland

We discuss the problem of fitting data points $\mathcal{Q}_m = \{q_i\}_{i=0}^m$ in arbitrary Euclidean space $\mathbb{E}^n$. It is additionally assumed here, that the corresponding interpolation knots $\{t_i\}_{i=0}^m$ remain unknown and as such they need to be somehow replaced by $\hat{\mathcal{T}} = \{\hat{t}_i\}_{i=0}^m$ (subject to $\hat{t}_i < \hat{t}_{i+1}$). Here, without loss of generality $\hat{t}_0 = 0$ and $\hat{t}_m = T$, for some $T > 0$. In the case of Q_m dense the issue of convergence rate of a given interpolation scheme $\hat{\gamma}$ (based on $\mathcal{Q}_m$ and $\hat{\mathcal{T}}$) in approximating γ (satisfying $\gamma(t_i) = q_i$) has been extensively studied (see e.g. [1]). In contrast for $\mathcal{Q}_m$ sparse a possible criterion to select the new knots $\hat{\mathcal{T}}$ is to minimize:

$$\mathcal{J}(\hat{t}_1, \hat{t}_2, \ldots, \hat{t}_{m-1}) = \int_0^T \|\ddot{\gamma}_N(\hat{t})\| d\hat{t}, \qquad (1)$$

where $\hat{\gamma}_N$ is a natural spline based on $\mathcal{Q}_m = \{q_i\}_{i=0}^m$ and $\hat{\mathcal{T}}$. Finding such optimal knots $\hat{\mathcal{T}}^{opt}$ forms a highly nonlinear optimization task (see e.g. [2]). One of the computational schemes handling (1) (called Leap-Frog) relies on the composition of overlapping univariate optimizations schemes - see [3]. We discuss special conditions under which the unimodality of these univariate functions holds and show the robustness in case of their perturbation.

Keywords
Interpolation, Optimization, Reduced Data

References

[1] R. Kozera, L. Noakes and M. Wiłołazka, Exponential parameterization to fit reduced data. *Applied Mathematics and Computation* **391**, 125645 (2021).
[2] R. Kozera and L. Noakes, Non-linearity and non-convexity in optimal knots selection for sparse reduced data. In V.P. Gerdt et al., *CASC 2017, LNCS* **10490**, 257-271 (2017).
[3] R. Kozera, L. Noakes and A. Wiliński, Generic case of Leap-Frog Algorithm for optimal knots selection in fitting reduced data. In M. Paszyński et al., *ICCS 2021, LNCS* **12745**, 337–350 (2021).

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *"Computer Algebra Modeling in Science and Engineering"*

Resonances and periodic motion of Atwood's machine with two oscillating bodies

Alexander Prokopenya[1] [alexander_prokopenya@sggw.edu.pl]

[1] Institute of Information Technology, Warsaw University of Life Sciences – SGGW, Warsaw, Poland

The swinging Atwood machine under consideration consists of two masses m_1, m_2 attached to opposite ends of a massless inextensible thread wound round two massless frictionless pulleys of negligible radius (see [1]). Both masses m_1 and m_2 are allowed to oscillate in a plane. Such a system has three degrees of freedom and its equations of motion may be written in the form

$$\begin{aligned} r\ddot{\varphi} &= -g\sin\varphi - 2\dot{r}\dot{\varphi}, \\ (L-r)\ddot{\psi} &= -g\sin\psi + 2\dot{r}\dot{\psi}, \\ (m_1+m_2)\ddot{r} &= m_1 g\cos\varphi - m_2 g\cos\psi + m_1 r\dot{\varphi}^2 - m_2(L-r)\dot{\psi}^2, \end{aligned} \tag{1}$$

where the dot above the symbol denotes a total time derivative of the corresponding function, the variables r, φ, ψ describe geometrical configuration of the system, g is a gravity constant. Note that equations of motion (1) are essentially nonlinear, and their general solution cannot be found in symbolic form. However, there exist periodic solutions which may be represented in the form of power series (see [2,3]). In the present talk, we construct such periodic solutions and demonstrate that they exist only if the frequencies of the bodies oscillations are commensurable or a resonance of frequencies takes place.

Keywords
Swinging Atwood machine, equations of motion, periodic solutions, resonances

References

[1] A.N. Prokopenya, Modelling Atwood's machine with three degrees of freedom. *Mathematics in Computer Science* **13**(1-2), 247–257 (2019).
[2] A.N. Prokopenya, Construction of a periodic solution to the equations of motion of generalized Atwood's machine using computer algebra. *Programming and Computer Software* **46**(2), 120–125 (2020).
[3] A.N. Prokopenya, Searching for equilibrium states of Atwood's machine with two oscillating bodies by means of computer algebra. *Programming and Computer Software* **47**(1), 43–49 (2021).

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *“Computer Algebra Modeling in Science and Engineering”*

Perturbations in the restricted three-body problem of variable mass

Alexander Prokopenya[1]***, Mukhtar Minglibayev***[2,3]
Aigerim Ibraimova[2,3] [alexander_prokopenya@sggw.edu.pl]

[1] Warsaw University of Life Sciences, Warsaw, Poland
[2] Al-Farabi Kazakh National University, Almaty, Kazakhstan
[3] Fesenkov Astrophysical Institute, Almaty, Kazakhstan

Real space systems are nonstationary, their masses, sizes, shapes changes in the process of evolution [1-3], as a result their mathematical models become more difficult. Modern computer algebra allows new symbolic computation algorithms for obtaining evolutionary equations. The restricted three-body problem with non-isotropically varying masses in the presence of reactive forces was investigated. Astronomical observations determine the reactive forces in the orbital coordinate system, so the perturbation theory in the form of Newton's equation was used [4]. The expansion of perturbing forces needs time-consuming and very cumbersome analytical calculations. We obtained expansions of the perturbing function in the orbital coordinate system. In the nonresonant case, averaging over the mean longitude, we obtained the equations of secular perturbation of the restricted three-body problem with variable masses in the presence of reactive forces. All analytical calculations are done in Wolfram Mathematica [5].

Keywords
restricted three-body problem, variable mass, reactive forces, secular perturbations

References

[1] T. OMAROV (ED.), *Non-Stationary Dynamical Problems in Astronomy*. Nova Science Publ., New-York, 2002.
[2] M. MINGLIBAYEV, *Dynamics of gravitating bodies with variable masses and sizes*. LAMBERT Academic Publishing, Saarbrücken, 2012.
[3] A. PROKOPENYA; M. MINGLIBAYEV; S. SHOMSHEKOVA, Computing Perturbations in the Two-Planetary Three-Body Problem with Masses Varying Non-isotropically at Different Rates. *Mathematics in Computer Science* **14**(2), 241–251 (2020).
[4] M. MINGLIBAYEV; CH. OMAROV; A. IBRAIMOVA, New forms of the perturbed motion equation. *RNAS RK* **2**(330), 5–13 (2020).
[5] S. WOLFRAM , *An Elementary Introduction to the Wolfram Language*. Wolfram Media, New York, 2016.

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *"Computer Algebra Modeling in Science and Engineering"*

Evolutionary equations in the two-planet three-body problem with variable masses

Alexander Prokopenya[1]***, Mukhtar Minglibayev***[2,3]***,***
Zhanar Imanova[4] [minglibayev@gmail.com]

[1] Warsaw University of Life Sciences, Warsaw, Poland
[2] Al-Farabi Kazakh National University, Almaty, Kazakhstan
[3] Fesenkov Astrophysical Institute, Almaty, Kazakhstan
[4] Korkyt Ata Kyzylorda University, Kyzylorda, Kazakhstan

Masses of real celestial bodies changes anisotropically [1-2]. Due to this the reactive forces appear, and they need to be taken into account in the study of the bodies dynamics. We studied the two-planet problem of three bodies with variable masses in the presence of reactive forces and obtained the equations of perturbed motion in the form of Newton's equations in the orbital coordinate system [3]. These equations are more convenient for taking into account the reactive forces than the Lagrange equations [4]. The perturbing forces are expanded in terms of osculating elements. The expansion of perturbing force is a time-consuming analytical calculation and results in very cumbersome analytical expressions. In the considered problem we obtained expansions of perturbing functions in powers of small parameters up to the second order. In the non-resonant case, we obtained the evolution equations in the Newton equation form. All symbolic calculations were performed with the Mathematica [5].

Keywords
two-planet three-body problem, variable mass, evolutionary equations.

References

[1] P. Eggleton, *Evolutionary processes in binary and multiple stars.* Cambridge University Press, New York, 2006.
[2] M. Minglibayev, *Dynamics of gravitating bodies with variable masses and sizes.* LAMBERT Academic Publishing, Saarbrücken, 2012.
[3] M. Minglibayev; Ch. Omarov; A. Ibraimova, New forms of the perturbed motion equation. *RNAS RK* **2**(330), 5–13 (2020).
[4] M. Minglibayev; A. Prokopenya; G. Mayemerova; Z. Imanova, Three-Body Problem with Variable Masses that Change Anisotropically at Different Rates. *Mathematics in Computer Science* **11**(3-4), 383—391 (2017).
[5] S. Wolfram, *An elementary introduction to the Wolfram Language.* Wolfram Media, 2016.

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *“Effective ideal theory and combinatorial techniques in commutative and non commutative rings and their applications”*

Generalized weights of codes via graded Betti numbers

Elisa Gorla[1] [elisa.gorla@unine.ch]

[1] Institut de Mathématiques, Université de Neuchâtel, Switzerland

In the past seventy years, much effort has been devoted to the study of algebraic and combinatorial objects associated to linear error-correcting codes. Of particular interest is the matroid associated to a linear code via its parity-check matrix, whose circuits are the minimal Hamming supports of the codewords. Many central results in classical coding theory, including the celebrated MacWilliams identities, their generalizations, and the duality between puncturing and shortening can be elegantly obtained via this correspondence, see e.g. [1,2,3,6] and the references therein.

The matroid associated to a linear code via its parity check matrix retains a wealth of information about the structure of the code, including its length, dimension, minimum distance, weight distribution, and generalized weights. In [5] it is shown that the code's generalized weights are determined by the graded Betti numbers of the Stanley-Reisner ideal of the matroid. The approach of [5] heavily relies on matroid theory and on the properties of the Hamming support.

In this talk, we report on a joint work with Alberto Ravagnani [4]. We consider the more general setting of R-linear codes $C \subseteq R^n$, where R is a finite commutative unitary ring. We propose a general definition of support as a function $\sigma : R^n \to \mathbb{N}^u$ that enjoys a few natural properties. This naturally extends the notion of Hamming support traditionally studied in coding theory [7, page 177]. We define the support of a code $C \subseteq R^n$ as the join of the supports of its elements.

We then define the generalized weights of a code via the supports of its subcodes. We identify a class of supports under which the algebra of the module R^n is compatible with the combinatorics of the poset $\mathbb{N}^u$ with the product order, which we call modular supports. As one might expect, the Hamming support is an example of a modular support.

Our main result connects the generalized weights of a code with the graded Betti numbers of a suitable monomial ideal. More precisely, we associate a monomial ideal to a code $C \subseteq R^n$ via the supports of its codewords. Under this correspondence, inclusion of supports translates into divisibility among monomials. Under suitable assumptions, the generalized weights of an R-linear code endowed with a modular support are determined by the graded Betti

numbers of the associated monomial ideal. This generalizes a result of [5], with a standalone proof that relies on commutative algebra, rather than on matroid theory.

Keywords
R-linear codes, generalized weights, graded Betti numbers.

References

[1] A. BARG, The matroid of supports of a linear code, *Applicable Algebra in Engineering, Communication and Computing* 8 (1997), no. 2, 165–172.

[2] T. BRITZ, Higher support matroids, *Discrete Mathematics* 307 (2007), no. 17-18, 2300–2308.

[3] T. BRITZ, Code enumerators and Tutte polynomials, *IEEE Transactions on Information Theory* 56 (2010), no. 9, 4350–4358.

[4] E. GORLA; A. RAVAGNANI, Generalized weights of codes over rings and invariants of monomial ideals, *preprint available at https://arxiv.org/abs/2201.05813*.

[5] T. JOHNSEN AND H. VERDURE, Hamming weights and Betti numbers of Stanley-Reisner rings associated to matroids, *Applicable Algebra in Engineering, Communication and Computing* 24 (2013), no. 1, 73–93.

[6] R. JURRIUS AND R. PELLIKAAN, Codes, arrangements and matroids, *Algebraic Geometry Modeling in Information Theory*, World Scientific, 2013, pp. 219–325.

[7] J. MACWILLIAMS AND N. SLOANE, The Theory of Error-Correcting Codes, *North-Holland Mathematical Library*, 1977.

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *"Effective ideal theory and combinatorial techniques in commutative and non commutative rings and their applications"*

Faster Change of Order Algorithm for Gröbner Bases Under Shape and Stability Assumptions

Jérémy Berthomieu[1]***, Vincent Neiger***[1]***, Mohab Safey El Din***[1] `[vincent.neiger@lip6.fr]`

[1] Sorbonne Université, CNRS, LIP6, F-75005 Paris, France

This talk reports on updates on a work published in the proceedings of ISSAC 2022 [2].

Solving zero-dimensional polynomial systems using Gröbner bases is usually done by, first, computing a Gröbner basis for the degree reverse lexicographic order, and next computing the lexicographic Gröbner basis with a change of order algorithm. Currently, despite the progress brought by [4, 3, 5], the change of order takes a significant part of the whole solving time on a wide range of problems (see [1, Tbl. 1]).

Like the fastest known change of order algorithms described in the above references, we will focus on the situation where the ideal defined by the system satisfies natural properties which can be recovered in generic coordinates. First, the ideal has a *shape* lexicographic Gröbner basis. Second, the set of leading terms with respect to the degree reverse lexicographic order has a *stability* property; in particular, the multiplication matrix of the smallest variable can be read on the input Gröbner basis.

The current fastest algorithms rely on the sparsity of this matrix. The improvement stems from the fact that this sparsity is actually a consequence of an algebraic structure, which is classically exploited to represent the matrix concisely as a univariate polynomial matrix [7, Sec. 9]. We show that the Hermite normal form of that matrix yields the sought lexicographic Gröbner basis, under assumptions which cover the shape position case. Under some mild assumption implying $n \leq t$, the arithmetic complexity of our algorithm is $\tilde{O}(t^{\omega-1}D)$, where n is the number of variables, t is a sparsity indicator of the aforementioned multiplication matrix, D is the degree of the zero-dimensional ideal under consideration, and ω is the exponent of matrix multiplication. This improves upon both state-of-the-art complexity bounds $\tilde{O}(tD^2)$ and $\tilde{O}(D^\omega)$, since $\omega < 3$ and $t \leq D$. Practical experiments, based on the `msolve` library [1] and the Polynomial Matrix Library [6], confirm the high practical benefit.

Keywords
Gröbner basis, polynomial system solving, change of monomial order, polynomial matrix, Hermite normal form.

References

[1] J. Berthomieu, C. Eder, and M. Safey El Din. Msolve: A library for solving polynomial systems. In *Proceedings ISSAC 2021*, pages 51–58. ACM, 2021. `https://msolve.lip6.fr/`.

[2] J. Berthomieu, V. Neiger, and M. Safey El Din. Faster Change of Order Algorithm for Gröbner Bases Under Shape and Stability Assumptions. In *Proceedings ISSAC 2022*, ACM, 2022.

[3] J.-C. Faugère, P. Gaudry, L. Huot, and G. Renault. Sub-Cubic Change of Ordering for Gröbner Basis: A Probabilistic Approach. In *Proceedings ISSAC 2014*, pages 170–177. ACM, 2014.

[4] J.-C. Faugère and C. Mou. Fast Algorithm for Change of Ordering of Zero-dimensional Gröbner Bases with Sparse Multiplication Matrices. In *Proceedings ISSAC 2011*, pages 115–122. ACM, 2011.

[5] J.-C. Faugère and C. Mou. Sparse FGLM algorithms. *J. Symb. Comput.*, 80(3):538–569, 2017.

[6] S. G. Hyun, V. Neiger, and É. Schost. Implementations of efficient univariate polynomial matrix algorithms and application to bivariate resultants. In *Proceedings ISSAC 2019*, pages 235–242. ACM, 2019. `https://github.com/vneiger/pml`.

[7] A. Storjohann. *Algorithms for Matrix Canonical Forms*. Phd thesis, Swiss Federal Institute of Technology – ETH, 2000.

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *"Effective ideal theory and combinatorial techniques in commutative and non commutative rings and their applications"*

Gröbner Bases and Tate Algebras of Varying Radii

***Xavier Caruso*[1],*Tristan Vaccon*[2], *Thibaut Verron*[3]** [tristan.vaccon@unilim.fr]

[1] Université de Bordeaux, CNRS, INRIA, Bordeaux, France
[2] Université de Limoges, CNRS, XLIM UMR 7252, Limoges, France
[3] Johannes Kepler University, Institute for Algebra, Linz, Austria

Tate series are a generalization of polynomials introduced by John Tate in 1962 [5], when defining a p-adic analogue of the correspondence between algebraic geometry and analytic geometry. This p-adic analogue is called rigid geometry, and Tate series, similar to analytic functions in the complex case, are its fundamental objects. Tate series are defined as multivariate formal power series over a p-adic ring or field, with a convergence condition on a closed ball given by a *convergence radius*.

Tate series are naturally approximated by multivariate polynomials over $\mathbb{F}_p$ or $\mathbb{Z}/p^n\mathbb{Z}$, and it is possible to define a theory of Gröbner bases for ideals of Tate series, which opens the way towards effective rigid geometry.

In [1, 2, 3], efforts have been made so that advanced algorithms to compute classical Gröbner bases (F4, F5, FGLM) can be adapted to Gröbner bases over Tate algebras.

In this talk, motivated by the phenomenon of overconvergence (series converging on a ball of larger convergence radius) and the local study of polynomial ideals, we will present algorithms we have developped in [3, 4] to handle a change of convergence radius of convergence (in case of overconvergence) and how to compute bases made of polynomial for an ideal in a Tate algebra spanned by polynomials.

Finally, we will present the concept of *universal analytic Gröbner basis* for a polynomial ideal: a finite polynomial basis of an ideal such that it is a Gröbner basis in any Tate algebra for any (rational) convergence radius.

Keywords
Algorithms, Gröbner bases, Tate algebra, Mora's algorithm, Universal Gröbner basis

References

[1] X. CARUSO; T. VACCON; T. VERRON, Gröbner bases over Tate algebras, In *Proceedings: ISSAC 2019, Beijing, China.*

[2] X. CARUSO; T. VACCON; T. VERRON, Signature-based algorithms for Gröbner bases over Tate algebras, In *Proceedings: ISSAC 2020, Kalamata, Greece.*

[3] X. CARUSO; T. VACCON; T. VERRON, On FGLM Algorithms With Tate Algebras, In *Proceedings: ISSAC 2021, Saint-Petersburg, Russia.*

[4] X. CARUSO; T. VACCON; T. VERRON, On Polynomial Ideals and Overconvergence in Tate Algebras, In *Proceedings: ISSAC 2022, Lille, France.*

[5] J. TATE, Rigid analytic spaces, In *Inventiones Mathematicae* **12**, 1971, 257–289

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *“Effective ideal theory and combinatorial techniques in commutative and non commutative rings and their applications”*

Duality, Trace Inversion Formula and Extreme Combinatorics: Yet another proof of Perles-Sauer-Shelah Lemma

Luis M. Pardo [luis.pardo@unican.es, luis.m.pardo@gmail.com]

Depto. de Matemáticas, Estadística y Computación. Facultad de Ciencias. Universidad de Cantabria. Avda. Los Castros s/n. E-39071 Santander, Spain.

This talk is just a modest contribution to prove several classical results in Extreme Combinatorics form the notions of Duality and Trace in some Artinian $K-$algebras (mainly through the Trace Inversion Formula), where K is a perfect field of characteristics not equal to 2. We prove how several classic combinatorial results are particular instances of a Trace Inversion formula in finite $\mathbb{Q}-$algebras. This is the case with the Exclusion-Inclusion Principle (in its general form, both with direct and reverse order associated to subsets inclusion). This approach also allows us to exhibit a basis of the space of null $t-$designs, which differs from the one described in Theorem 4 of [1]. Inspired and motivated by the proof in [2] of the Perles-Sauer-Shelah Lemma (cf. [3], [4]), we produce a new one based only in Duality and Trace in a $\mathbb{Q}-$algebra $\mathbb{Q}[V_n]$, which we introduced ad hoc. All results are equally true if we replace $\mathbb{Q}[V_n]$ by $K[V_n]$, where K is any perfect field of characteristics $\neq 2$. We have tried to be as self-contained and elementary as possible, trying to make this material accessible to a wide mathematical audience.

Keywords
Tace, Duality, Learning, Extreme Combinatorics, Perles-Sauer-Shelah Lemma,

References

[1] M. DEZA, P. FRANKL, *On the vector space of 0-configurations.* Combinatorica **2** (1982), 341-345.
[2] P. FRANKL, J. PACH, *On the number of sets in a null t-design.* European J. Combinatorics **4** (1983), 21-23.
[3] N. SAUER, *On the density of families of sets*. J. of Combinatorial Theory, Series A, **13** (1972), 145–147.
[4] S. SHELAH, *A combinatorial problem; stability and order for models and theories in infinitary languages*. Pacific J. of Mathematics **41** (1972) 247–261.

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *“Computational Differential and Difference Algebra and its Applications”*

Solving degree and last fall degree

Alessio Caminata[1]***, Elisa Gorla***[2] [caminata@dima.unige.it]

[1] Dipartimento di Matematica, Università di Genova, Genova, Italy
[2] Institut de Mathématiques, Université de Neuchâtel, Neuchâtel, Switzerland

As computational problems can often be modelled via polynomial equations, several security estimates in Cryptography depend on the complexity of polynomial system solving. The solutions of a system of polynomial equations over a finite field can be computed in polynomial time from a lexicographic Gröbner basis of the system. Nowadays, the most efficient algorithms to compute Gröbner bases belong to the family of linear-algebra-based algorithms, for example F4/F5 and the family of XL Algorithms. The complexity of these algorithms is bounded from above by a known function of the **solving degree**, which is the highest degree of the polynomials appearing during the computation. However, finding the solving degree of a system without computing its Gröbner basis is often hard. This motivated the introduction of several algebraic invariants related to the solving degree. One such invariant is the **last fall degree** introduced by Huang, Kosters, Yang, and Yeo.

In this talk, I will discuss some equivalent definitions for the last fall degree and provide a new one that involves the concept of degree falls. Moreover, I will discuss the relation between solving degree and last fall degree and I will show that for any degree-compatible term order, the solving degree of a system is the maximum between its last fall degree and the largest degree of an element in a reduced Gröbner basis of the system. This provides a proof for the intuitive fact that the two key ingredients in determining the solving degree of a system are the degrees of the elements in its reduced Gröbner basis and the degree falls.

Keywords
solving degree, last fall degree, Gröbner basis

References

[1] A. Caminata, E. Gorla, *Solving degree, last fall degree, and related invariants*. To appear in: Journal of Symbolic computation, `https://doi.org/10.1016/j.jsc.2022.05.001`

[2] M.-D. A. Huang, M. Kosters, Y. Yang, S. L. Yeo, *On the last fall degree of zero-dimensional Weil descent systems*, Journal of Symbolic computation **87** (2018), 207–226.

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *“Effective ideal theory and combinatorial techniques in commutative and non commutative rings and their applications”*

Noncommutative Novikov algebras

Pavel Kolesnikov[1] [pavelsk77@gmail.com]

[1] Sobolev Institute of Mathematics, Novosibirsk, Russia

The variety of Novikov algebras appeared in the paper [1] devoted to the study of Poisson brackets of hydrodynamic type, though it emerged earlier in [2] as a tool for constructing Hamiltonian operators in formal variational calculus. The axioms of Novikov algebras appear in [1] as necessary and sufficient conditions for the local algebra of a formal Poisson bracket to meet the Jacobi identity.

Let us state the corresponding construction in a “coordinate-free” form. Suppose V is a non-associative algebra over a field $\Bbbk$ with a bilinear product $\circ$, and A is the algebra of smooth functions in one variable z. Consider the space $A \otimes V$ equipped with a skew-symmetric bilinear operation $[\cdot,\cdot]$ given by

$$[a(z)\otimes v, b(z)\otimes w] = a'(z)b(z)\otimes (v\circ w) - b'(z)a(z)\otimes (w\circ v),$$

$a,b \in A$, $v,w \in V$. Then $[\cdot,\cdot]$ is a Lie bracket if and only if the algebra $(V,\circ)$ meets the following relations for all $u,v,w\in V$:

$$(u\circ v)\circ w = (u\circ w)\circ v, \quad (u,v,w)_\circ = (v,u,w)_\circ,$$

where $(x,y,z)_\circ = (x\circ y)\circ z - x\circ(y\circ z)$. These two identities define the variety of Novikov algebras.

A series of examples of Novikov algebras may be constructed as follows [2]. For an associative and commutative algebra V with a derivation d, let $u\circ v = ud(v)$, for $u,v\in V$. Then $(V,\circ)$ is a Novikov algebra.

This construction is known to be generic [3], i.e., every Novikov algebra embeds into an appropriate commutative algebra with a derivation. The proof of this statement in [3] is based on the Gröbner–Shirshov bases theory for Novikov algebras, the latter essentially uses the fundamental result of [4], where it was shown that the free Novikov algebra $\mathrm{Nov}(X)$ generated by a set X embeds into the algebra of differential polynomials in X. However, modulo this fact from [4], the embedding of an arbitrary Novikov algebra into a commutative differential algebra may be proved in a shorter way (see [5]). Therefore, the result of [4] (which is mostly combinatorial) still plays a key role in the theory of Novikov algebras.

The embedding of the free Novikov algebra into the free commutative differential algebra is an essential part of the general theory on identities of derived algebras. Suppose A is a (non-associative, in general) algebra with multiplication $\mu(x,y) = xy$, and let d be a derivation of A. Then the same space A equipped with two new operations

$$x \succ y = d(x)y, \quad x \prec y = xd(y), \quad x, y \in A,$$

is said to be a derived algebra of A. For example, for every associative and commutative algebra A ($A \in \mathrm{Com}$), its derived algebra is a Novikov one (note that $x \succ y = y \prec x$ in the commutative case). The result of [4] on the free Novikov algebra states that there are no more (independent) identities that hold on all derived commutative algebras apart from the identities of Novikov algebras.

Let Var be a variety of linear algebras with binary operations $\mu_i(x,y) = x \cdot_i y$, $i \in I$, the corresponding (symmetric) binary operad is denoted by the same symbol Var. In particular Nov, is the operad of Novikov algebras generated by one binary operation $\mu(x,y) = x \circ y$. Let us denote by $D\mathrm{Var}$ the variety of algebras with duplicated family of operations

$$\mu_i^{\succ}(x,y) = x \succ_i y, \quad \mu_i^{\prec}(x,y) = x \prec_i y, \quad i \in I,$$

defined by all those identities that hold for all Var-algebras with a derivation d relative to the operations

$$x \succ_i y = d(x) \cdot_i y, \quad x \prec_i y = x \cdot_i d(y).$$

As it was shown in [6], the operad $D\mathrm{Var}$ is isomorphic to the Manin white product of Var and Nov, so that $\mu_i^{\succ} = \mu_i \otimes \mu^{(12)}$, $\mu_i^{\prec} = \mu_i \otimes \mu$.

In particular, for $\mathrm{Var} = \mathrm{As}$ (the variety of associative algebras), the identities that hold on $D\mathrm{As}$ were found by J.-L. Loday [7]:

$$\begin{gathered} x \succ (y \prec z) = (x \succ y) \prec z, \\ (x \prec y) \succ z - x \succ (y \succ z) = x \prec (y \succ z) - (x \prec y) \prec z. \end{gathered} \tag{1}$$

The general result on $D\mathrm{Var}$ implies that there are no more independent identities on $D\mathrm{As}$, and it is not hard to derive that every $D\mathrm{As}$ algebra embeds into an appropriate associative differential algebra. The keystone of the proof is again the result of [4] on free Novikov algebras.

Our purpose was to find a straightforward way to prove the embedding of a $D\mathrm{As}$-algebra into an appropriate associative differential algebra by means of the (differential) Gröbner–Shirshov bases theory. In particular, restricting to the commutative algebras and their Gröbner bases, we get an independent proof the embedding of a Novikov algebra into a commutative differential algebra.

On the one hand, Gröbner and Gröbner–Shirshov bases are the tools that are especially designed for solving such embedding problems. Given a Novikov algebra V with a linear basis X and multiplication table S, let us construct the algebra F of polynomials in $X \cup X' \cup X'' \cup \cdots \cup X^{(n)} \cup \ldots$ with a derivation $d : x^{(n)} \mapsto x^{(n+1)}$, $x \in X$, and find the differential ideal I generated by the polynomials

$$xy' - f_{xy}, \quad x, y \in X,$$

where f_{xy} is the linear form in X equal to $x \circ y$ in V. The quotient F/I is the "universal differential envelope" of V, so it remains to show that nonzero linear forms do not belong to I, i.e., $V \subseteq F/I$.

On the other hand, the explicit calculation of the Gröbner basis (relative to a chosen order of monomials) for the ideal I highly depends on the particular multiplication table S. For example, the composition of $xy' - f_{xy}$ and $zy' - f_{zy}$ relative to the natural deg-lex order is equal to $zf_{xy} - xf_{zy}$, and the principal part can be determined by the particular form of f. In other words, the pair $(\mathrm{Nov}, \mathrm{ComDer})$ has no PBW-property in the sense of [8], and the same holds for the pair $(D\mathrm{As}, \mathrm{AsDer})$.

We present a way how to overcome this problem. Suppose V is a DAs-algebra with operations $\succ$, $\prec$, and let X be a basis of V. Working in the noncommutative setting, construct the free associative algebra F as above, and define I to be the differential ideal generated by

$$xy' - (x \prec y), \quad x'y - (x \succ y), \quad x, y \in X.$$

Although it is hard to control the corresponding rewriting system $\mathcal{G}$ in general, we may choose a subgraph $\mathcal{G}_{-1}$ whose vertices are weight-homogeneous noncommutative polynomials of weight -1 (the weight of a monomial $x_1^{(i_1)} \dots x_n^{(i_n)}$ is set to be $i_1 + \dots + i_n - n$).

It turns out that $\mathcal{G}_{-1}$ is a confluent rewriting system for every DAs-algebra V. Hence, every algebra that meets the identities (1) embeds into an associative differential algebra.

Keywords
Derivation, Novikov algebra, Gröbner basis

References

[1] A. A. Balinskii, S. P. Novikov, Poisson brackets of hydrodynamic type, Frobenius algebras and Lie algebras. *Sov. Math. Dokl.* **32**, 228–231 (1985).

[2] I. M. Gelfand, I. Ya. Dorfman, Hamilton operators and associated algebraic structures. *Functional analysis and its application* **13**(4), 13–30 (1979).

[3] L. A. Bokut, Y. Chen, Z. Zhang, Gröbner–Shirshov bases method for Gelfand–Dorfman–Novikov algebras. *J. Algebra Appl.* **16**(1), 1750001, 22 pp. (2017).

[4] A. S. Dzhumadil'daev, C. Löfwall, Trees, free right-symmetric algebras, free Novikov algebras and identities. *Homology, Homotopy Appl.* **4**(2), 165–190 (2002).

[5] P. S. Kolesnikov, B. Sartayev, On the Special Identities of Gelfand–Dorfman Algebras *Experimental Math.*, to appear,

[6] P. S. Kolesnikov, B. Sartayev, A. Orazgaliev, Gelfand–Dorfman algebras, derived identities, and the Manin product of operads. *Journal of Algebra* **539**, 260–284 (2019).

[7] J.-L. Loday, On the operad of associative algebras with derivation. *Georgian Math. J.* **17**(2), 347–372 (2010).

[8] A. A. MIKHALEV, I. P. SHESTAKOV, PBW-pairs of varieties of linear algebras. *Comm. Algebra* **42**(2), 667–687 (2014).

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *"Effective ideal theory and combinatorial techniques in commutative and non commutative rings and their applications"*

Discrete Vector Fields for Monomial Resolutions

Eduardo Sáenz-de-Cabezón[1]***, Francis Sergeraert***[2] [esaenz-d@unirioja.es]

[1] Departamento de Matemáticas y Computación, Universidad de La Rioja, Spain
[2] Université de Grenoble- Alpes and Université Bretagne Sud., France

The construction and computation of minimal free resolutions of monomial ideals is a central problem in combinatorial commutative algebra. There is a large body of research on the topic that has led to extensive literature on monomial resolutions. The two main lines of research on this subject consist, on the one hand, in finding explicit minimal free resolutions for particular families of monomial ideals and, on the other hand, in finding general procedures to obtain free resolutions that (although possibly not minimal) provide homological information on the ideal.

The main result of the first approach is the explicit description of the minimal free resolution of stable ideals given by Eliahou and Kevaire [5]. Squarefree versions of this were given in [3, 7]. In [13], Seiler gave a (non-minimal) explicit free resolution for quasi-stable ideals based on the work of Eliahou and Kervaire. The main construction within the second approach is the Taylor resolution [15], which is a combinatorial explicit resolution that is usually not minimal. A more compact resolution derived from this was given by Lyubeznik [11]. Taylor and Lyubeznik resolutions are two instances of *cellular resolutions* [4], which take advantage of the combinatorial nature of monomial ideals to encode their resolutions by means of cellular complexes. As a complement to this line of research, several techniques for minimizing a given resolution have been developed, in particular those based on those based on Discrete Vector Fields (a subject initiated by R. Forman in [6], satellite of his Discrete Morse Theory), see [2] for a recent example. Another general technique for constructing monomial resolutions is the iterated mapping cone [10], which allows the construction of (non-minimal) free resolutions for arbitrary polynomial and monomial ideals. For instance, the already mentioned Taylor, Eliahou-Kervaire and Pommaret-Seiler resolutions are examples of iterated mapping cones.

The computational aspects of the problem, i.e. the explicit computation of monomial resolutions, in particular the minimal one and the invariants related to it have also received much attention [14, 12] and the main computer algebra systems focused on commutative algebra have algorithms to construct minimal free resolutions [1, 8, 9].

Our contribution is the following. We develop an effective version of the iterated mapping

cone approach that makes it completely constructive, avoiding in this way the limitations of the method, as expressed in [10]. We use discrete vector fields to explicitly iterate on the mapping cone construction so that an actual algorithm can be built from it for any monomial ideal. Furthermore, we use Discrete Vector Fields to minimize the iterated mapping cone resolution. This reduction step, can however be applied to any monomial resolution. We also build algorithms to construct free resolutions of monomial ideals based on these results and give details on the implementation.

Keywords
Discrete vector fields, monomial resolutions, mapping cone

References

[1] J. Abbott and A. M. Bigatti. CoCoALib: a C++ library for doing Computations in Commutative Algebra. Available at `http://cocoa.dima.unige.it/cocoalib`.

[2] J. Àlvarez-Montaner, O. Fernández-Ramos, and P. Gimenez. Pruned cellular free resolutions of monomial ideals. *Journal of Algebra*, 541:126–145, 2020.

[3] A. Aramova, J. Herzog, and T. Hibi. Squarefree lexsegment ideals. *Math. Z.*, 228(2):353–378, 1998.

[4] D. Bayer and B. Sturmfels. Cellular resolutions of monomial modules. *J. Reine Angew. Math.*, 502:123–140, 1998.

[5] S. Eliahou and M. Kervaire. Minimal resolutions of some monomial ideals. *Journal of Algebra*, 129:1–25, 1990.

[6] R. Forman. Morse theory for cell complexes. *Advances in Mathematics*, 134:90–145, 1998.

[7] V. Gasharov, T. Hibi, and I. Peeva. Resolutions of a-stable ideals. *Journal of Algebra*, 254(2):375–394, 2002.

[8] Daniel R. Grayson and Michael E. Stillman. Macaulay2, a software system for research in algebraic geometry. Available at http://www.math.uiuc.edu/Macaulay2/.

[9] G.-M. Greuel, G. Pfister, and H. Schönemann. SINGULAR 3-1-0 — A computer algebra system for polynomial computations. 2009. http://www.singular.uni-kl.de.

[10] J. Herzog and Y. Takayama. Resolutions by mapping cones. *Homology, Homotopy and Applications*, 4(2):277–294, 2002.

[11] G. Lyubeznik. A new explicit finite free resolution of ideals generated by monomials in an r-sequence. *J. Pure and Appl. Algebra*, 51:193–195, 1988.

[12] E. Sáenz de Cabezón. Multigraded Betti numbers without computing minimal free resolutions. *Applicable Algebra in Enigineering, Communication and Computing*, 10:1–2, 2009.

[13] Werner M. Seiler. A combinatorial approach to involution and δ-regularity ii: Structure analysis of polynomial modules with Pommaret bases. *Applicable Algebra in Engineering, Communications and Computing*, 20:261–338, 2009.

[14] T. Siebert. Recursive computation of free resolutions and a generalized Koszul complex. *Applicable Algebra in Engineering, Communication and Computing*, 14:133–149, 2003.

[15] D. Taylor. *Ideals generated by monomials in an R-sequence*. PhD thesis, University of Chicago, 1966.

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *“Computational Differential and Difference Algebra and its Applications”*

Private Distributed Coded Computation

Malihe Aliasgari[1]***, Yousef Nejatbakhsh***[2]

[1]New Jersey Center for Science, Technology and Mathematics (NJCSTM), Kean University, New Jersey, USA [maliasga@kean.edu]
[2]Department of Mathematics, Caldwell University, New Jersey, USA
[yousef.nejatbakhsh@njit.edu]

The era of Big Data and the immensity of real-life datasets compels computation tasks to be performed in a distributed fashion, where the data is dispersed among many servers that operate in parallel [1,2]. However, massive parallelization leads to computational bottlenecks due to faulty servers and stragglers. The key idea is that, by employing suitable linear codes operating over fractions of the original data, a function may be completed as soon as enough number of processors, depending on the minimum distance of the code, have completed their operations.

In this talk we consider the problem of secure and private distributed matrix multiplication in a big size and present the trade-off between communication load and recovery threshold.

Keywords
Coding Theory, coded computation, privacy

References

[1] S. Li; M. A. Maddah-Ali; Q. Yu; A. S. Avestimehr, *A fundamental tradeoff between computation and communication in distributed computing*. In: *IEEE Transactions on Information Theory.*, **volume** 65, 2018.

[2] M. Aliasgari; O. Simeone; J. Kliewer, *Distributed and private coded matrix computation with flexible communication load.* In: *IEEE Transactions on Information Forensics and Security*, **volume** 65, 109–1287, 2020.

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *"Effective ideal theory and combinatorial techniques in commutative and non commutative rings and their applications"*

Algebraic, Geometric, and Combinatorial Aspects of Unique Model Identification

Brandilyn Stigler[1] [bstigler@smu.edu]

[1] Department of Mathematics, Southern Methodist University, Dallas, Texas, USA

Biological data science is a field replete with many substantial data sets from laboratory experiments and myriad diverse methods for analysis and modeling. Given the abundance of both data and models, there is a growing need to group data sets to reveal salient features of the data and untimely of the underlying network. For discrete data, that is n-tuples with entries in a finite field F, a special class of discrete models called *polynomial dynamical systems* can be used to capture all models which fit the given data from a network with n nodes. Specifically a *polynomial dynamical system* over F is a polynomial map $f : F^n \to F^n$ where $f = (f_1, \dots, f_n)$ and each coordinate function $f_i : F^n \to F$ is a polynomial in $F[x_1, \dots, x_n]$. We say that f *fits* the input-output data $D = \{(s_1, t_1), \dots, (s_m, t_m)\} \subset F^n \times F^n$ if $f(s_j) = t_j$ for each $1 \leq j \leq m$. Typically a data set can have a large number of associated models, requiring model selection. In the face of limited understanding of the underlying network, selecting models which accurately reflect the network can be challenging.

A key question is to identify data sets which guarantee a unique polynomial dynamical system. The problem translates mathematically to identifying input sets $V \subset F^n$ such that the associated quotient ring $F[x_1, \dots, x_n]/\mathbb{I}(V)$ has a unique basis (up to scalar multiple) as a vector space over F. For data sets corresponding to a large number of bases, finding all bases may be cumbersome. Gröbner bases offer an *algorithmic* solution, albeit an incomplete one: while not all bases of the quotient ring are compatible with a monomial order, all the ones that are can be found algorithmically. The advantage of this strategy is that one can view all possible bases of the quotient ring to select those that are the most biologically relevant. Hence the revised problem we consider is identifying input data sets with an ideal of points $\mathbb{I}(V)$ having a unique reduced Gröbner basis (URGB) for any monomial ordering.

In this talk we show a necessary and sufficient condition on $\mathbb{I}(V)$ that guarantees that it has a URGB. In fact it is an algebraic property on the generators of $\mathbb{I}(V)$ that can be easily checked [2]. We also summarize two distinct sufficient conditions on the input data V so that $\mathbb{I}(V)$ has a URGB: if V is the linear shift of a staircase (a geometric property) [1] and if V is the variety of the distraction of some monomial ideal (an algebraic property) [2]. Since we are were interested in grouping data which facilitates model selection, we used linear shifts to partition data into equivalence classes and showed that each equivalence class has an associated collection of (standard monomial) bases [3].

Next we relax the condition of requiring a unique polynomial dynamical system and focus on identifying data sets with a unique *wiring diagram*, that is a directed graph on n nodes representing the connections in the network. While the wiring diagram represents only a static picture of the network, knowledge of the connectivity is crucial for studying network robustness, regulation, and control strategies.

For each node x_r in the network, consider the data for x_r: $D_r = \{(s_1, t_1), \dots, (s_m, t_m)\} \subset F^n \times F$; notice that each t_i is now a scalar. For every pair of distinct input n-tuples $s_i = (s_{i1}, \dots, s_{in})$ and $s_j = (s_{j1}, \dots, s_{jn})$ with distinct corresponding output values ($t_i \neq t_j$), we can encode the coordinates in which they differ by a square-free monomial

$$m(s_i, s_j) = \prod_{s_{ik} \neq s_{jk}} x_k.$$

Let $\mathcal{M}$ be the ideal generated by all such monomials, that is,

$$\mathcal{M} = \langle m(s_i, s_j) \mid s_i \neq s_j, t_i \neq t_j \rangle.$$

We call the generators of the associated primes in its primary decomposition the *minimal sets* of x_r. Each set of generators is a list of variables representing the incoming edges to x_r in the wiring diagram. Furthermore each set has the property that there exists a polynomial in those variables that fits the data in D_r and there is no such polynomial for any proper subset.

We present a couple of algebraic conditions on $\mathbb{I}(V)$, where V is the set of inputs as before, that each guarantees that there is a *unique* minimal set. We also provide a geometric condition on the data that guarantees the existence of *multiple* minimal sets. This is ongoing joint work with E. Dimitrova, C. Fredrickson, N. Rondoni, and A. Veliz-Cuba.

These results increase the utility of polynomial dynamical systems as models of complex networks by establishing the minimal amount of the data for unique model identification.

Keywords
Finite fields, Ideals of points, Gröbner bases

References

[1] Q. He, E. Dimitrova, B. Stigler, AND A. Zhang, Geometric characterization of data sets with unique reduced Gröbner bases. *Bulletin of Mathematical Biology* **81** 2691–2705 (2019).
[2] E. Dimitrova, Q. He, L. Robianno, B. Stigler. Small Gröbner fans of ideals of points. *Journal of Algebra and its Applications* (2019).
[3] A. Zhang, J. Hu, Q. Liang, E. Dimitrova, B. Stigler. Algebraic model selection and experimental design in biological data science. *Advances in Applied Mathematics* **133** (2021).

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *"Effective ideal theory and combinatorial techniques in commutative and non commutative rings and their applications"*

On computing isomorphisms between algebraic number fields

Michael Monagan[1] [mmonagan@sfu.ca]

[1] Department of Mathematics, Simon Fraser University, Vancouver, Canada

Let $K = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_k)$ be an algebraic number field. For example $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Then K is a vector space over $\mathbb{Q}$. Let $d = \dim(K : \mathbb{Q})$. Without loss of generality we assume $\mathbb{Q}(\alpha_1, \ldots, \alpha_i)$ is a proper subfield of $\mathbb{Q}(\alpha_1, \ldots, \alpha_i, \alpha_{i+1})$ for $1 \leq 1 < k$.

Let $c_1, c_2, \ldots, c_k$ be integers and let $\gamma = \sum_{i=1}^{k} c_i \, \alpha_i$. For almost all c_i we have $K \simeq \mathbb{Q}(\gamma)$. In this work we want to compute the field isomorphism $\varphi : K \to \mathbb{Q}(\gamma)$ as fast as possible.

Our motivation is the modular GCD algorithm of van Hoeij and Monagan from [3]. For two polynomials $A, B \in K[x]$ their algorithm computes $G = \gcd(A, B)$ modulo a sequence of primes $p_1, p_2, \ldots$, then applies the Chinese remainder theorem to compute G modulo m where m is the product of primes, and then uses Wang's rational number reconstruction from [4] to recover the rational coefficients of G from their images modulo m. The speed of their algorithm depends on the speed of arithmetic in K modulo a prime p.

How do we represent the elements of K and K mod p and how do we do arithmetic in K and in K mod p? The approach taken by the computer algebra systems Pari and Maple is to construct K as a sequence of quotients (see below) and use a recursive polynomial data structure to represent the elements of K.

```
Set $K_0 = \mathbb{Q}$.
For $i = 1$ to $k$ do
    Let $m_i(z_i)$ be the minimal polynomial for $\alpha_i$ over $K_{i-1}$ and let $d_i = \deg(m_i, z_i)$.
    Set $K_i = K_{i-1}[z_i]/\langle m_i \rangle$.
```

We have $K \simeq K_k$ and $d = \prod_{i=1}^{k} d_i$. Also K is isomorphic to the quotient ring $R = \mathbb{Q}[z_1, \ldots, z_k]/I$ where I is the ideal $\langle m(z_1), \ldots, m(z_k) \rangle$.

One way to do arithmetic in R would be to represent elements of R as sparse multivariate polynomials in $\mathbb{Q}[z_1, z_2, \ldots, z_k]$ and use Gröbner bases. We have $\{m_1, m_2, \ldots, m_k\}$ is a

Gröbner basis for I in lexicographical order with $z_1 < z_2 < \cdots < z_k$. However, this is expensive as a multiplication in R will do many multivariate polynomial operations.

Pari represents multivariate polynomials recursively, that is, Pari thinks of a polynomial in $\mathbb{Q}[z_1, z_2, \ldots, z_k]$ as a polynomial in $\mathbb{Q}[z_1][z_2]\cdots[z_k]$ and it uses a dense recursive polynomial data structure so that it needs univariate polynomial arithmetic only. Inspired by Pari's representation, van Hoeij and Monagan [3] also used a dense recursive representation for polynomials for their Maple implementation of the modular GCD algorithm in $K[x]$. For example, the polynomial $7x^2 + 5z_2^2 + 3z_1^2$ in $\mathbb{Q}[z_1][z_2][x]$ is stored as the Maple list of lists of lists of integers `[[[0,0,3],0,[5]],0,[[7]]]`.

We have observed that when $k > 1$ and m_1 has low degree, which is often the case practice, it is faster (typically 5 to 10 times faster) to multiply in $\mathbb{Q}(\gamma)$ mod p than to multiply in K mod p. One reason for this is that to multiply in K_3 mod p we do many multiplications in K_2 mod p, each of which does many multiplications in K_1, each of which requires memory to be allocated for the intermediate product and several function calls. This overhead is minimized when $k = 1$. In our talk we will present timing data to measure the overhead in Pari, Maple and Magma. **Thus our hypothesis:** to compute $\gcd(A, B)$ mod p, for $\deg(A, x)$ and $\deg(B, x)$ sufficiently large, it should be faster if we first compute φ mod p and map the GCD computation from K mod p into $\mathbb{Q}(\gamma)$ mod p.

How do we compute the isomorphism $\varphi : K \to \mathbb{Q}(\gamma)$? In our talk we present three methods (sketched below) to compute φ. The first method uses Gröbner bases, the second uses Linear Algebra, and the third uses iterated resultants. We have implemented the second method in C modulo a prime p. Our C implementation uses a dense recursive representation for elements of K mod p and supports primes up to 63 bits. We present timings for computing GCDs in $K[x]$ mod p comparing Pari, Magma, and Maple with our C code.

Method 1: Gröbner Bases.

Let $\gamma = \sum_{i=1}^{k} c_i z_i$ and let $m(z)$ be the minimal polynomial for γ over $\mathbb{Q}$. Let

$$F = [m_1(z_1), \ldots, m_k(z_k), z - \gamma]$$

and let G be the reduced Gröbner basis for F in lexicographical order with $z < z_1 < \cdots < z_k$. For almost all c_i we have $G \cap \mathbb{Q}[z] = \{m(z)\}$ and the remaining elements of G give us $\varphi(z_i)$. We give an example to illustrate.

Example 1. For $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ we have $m_1(z_1) = z_1^2 - 2$ and $m_2(z_2) = z_2^2 - 3$ and a basis for K over $\mathbb{Q}$ is $[1, z_1, z_2, z_1 z_2]$. For $c_1 = c_2 = 1$ we have $\gamma = z_1 + z_2$ and $F = [z_1^2 - 2, z_2^2 - 3, z - z_1 - z_2]$. We obtain the Gröbner basis

$$G = [z^4 - 10z^2 + 1, z_1 + \tfrac{9}{2}z - \tfrac{1}{2}z^3, z_2 - \tfrac{11}{2}z + \tfrac{1}{2}z^3].$$

Thus $m(z) = z^4 - 10z^2 + 1$, $\varphi(z_1) = -\frac{9}{2}z + \frac{1}{2}z^3$ and $\varphi(z_2) = \frac{11}{2}z - \frac{1}{2}z^3$. We have $\varphi(1) = 1$ and we compute $\varphi(z_1 z_2) = \varphi(z_1)\varphi(z_2)$.

Notice that F is also a Gröbner basis for the ideal generated by F in lexicographical order with $z_1 < z_2 < \cdots < z_k < z$ because the leading monomials of the polynomials in F are

$z_1^{d_1}, z_2^{d_2}, \ldots, z_k^{d_k}$ and z which are all relatively prime! Therefore, we may compute G from F using FGLM, the Gröbner basis conversion algorithm of Faugere, Gianni, Lazard and Mora [2]. The FGLM algorithm does $O(kd^3)$ arithmetic operations in $\mathbb{Q}$.

Method 2: Linear Algebra.

The number field $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_k)$ is a vector space over $\mathbb{Q}$. Let $d = \dim(K : \mathbb{Q})$ and let $m(z) = z^d + \sum_{i=0}^{d-1} x_i z^i$ be the minimal polynomial for γ over $\mathbb{Q}$ for x_i unknown. Equating $m(\gamma) = 0$ we obtain a linear system $\sum_{i=0}^{d-1} x_i \gamma^i = -\gamma^d$. In matrix form we have $Ax = b$ where $A = [\,1\,|\,\gamma\,|\,\gamma^2\,|\ldots|\,\gamma^{d-1}\,]$ and $b = -\gamma^d$. We construct A then invert A and obtain x from $x = A^{-1}b$. The matrix A^{-1} is the mapping $\varphi : K \to \mathbb{Q}(\gamma)$ thus A gives us φ^{-1}. Method 2 does $O(d^3)$ arithmetic operations in $\mathbb{Q}$.

Method 3: Iterated Resultants.

Let $\gamma = \sum_{i=1}^{k} c_i z_i$. Starting with the polynomial $z - \gamma$ we use the subresultant algorithm (see [4]) to first use m_k to eliminate z_k then to use m_{k-1} to eliminate z_{k-1}, etc., until we have eliminated all z_i and we obtain the minimal polynomial $m(z)$. In a second stage we successively obtain $\varphi(z_1)$, $\varphi(z_2)$, ..., $\varphi(z_k)$ using the penultimate polynomials in the subresultant remainder sequences which are linear for almost all c_i.

Example 1 (continued). First we apply the subresultant algorithm to $z - z_1 - z_2$ and $z_2^2 - 2$ to eliminate z_2. We obtain 3 polynomials $z_2^2 - 2$, $z - z_1 - z_2$ (which is linear in z_2) and $-2zz_1 + z^2 + 1$. Next we apply the subresultant algorithm to $-2zz_1 + z^2 + 1$ and $z_1^2 - 3$ to eliminate z_1. We obtain 3 polynomials $z_1^2 - 3$, $-2zz_1 + z^2 + 1$ (which is linear in z_1) and $z^4 - 10z^2 + 1$ (the minimal polynomial for γ).

Now we compute $\varphi(z_1)$ by solving $-2zz_1 + z^2 + 1 = 0$ for $z_1 \bmod m(z)$. We must invert $-2z$ in $\mathbb{Q}[z]/\langle m(z) \rangle$ using he Euclidean algorithm. We then solve $z - \varphi(z_1) - z_2 = 0$ for z_2 to determine $\varphi(z_2)$. Finally we compute $\varphi(z_1 z_2) = \varphi(z_1)\varphi(z_2)$.

Method 3 also does $O(d^3)$ arithmetic operations in $\mathbb{Q}$. But unlike methods 1 and 2 which solve linear systems of size $d \times d$, it only does polynomial arithmetic. We are currently investigating whether we can accelerate method 3.

Keywords
Grobner Bases, Algebraic number fields, Polynomial GCD, Field isomorphisms, Resultants

References

[1] B. Buchberger, G.E. Collins, R. Loos, R. Albrecht. *Computer Algebra*. Springer, 1983.

[2] J.C. Faugere, P. Gianni, D. Lazard, T. Mora. Efficient Computation of Zero-dimensional Gröbner Bases by Change of Ordering. *J. Symb. Comp.* **16**(4), 329–344 (1993).

[3] M. van Hoeij, M. Monagan., A Modular GCD Algorithm over Number Fields Presented with Multiple Field Extensions. In *Proceedings of ISSAC '02*, 109–116. ACM, 2002.

[4] P. WANG. A p-adic algorithm for univariate partial fractions. In *Proceedings of SYMSAC '81*, 212–217, ACM, 1981.

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *"Effective ideal theory and combinatorial techniques in commutative and non commutative rings and their applications"*

Linear Label Code of a Lattice Using Gröbner bases

Malihe Aliasgari[1], ***Daniel Panario***[2], ***Mohammad-Reza Sadeghi***[3]

[1] New Jersey Center for Science, Technology and Mathematics (NJCSTM), Kean University, New Jersey, USA [maliasga@kean.edu]
[2] School of Mathematics and Statistics, Carleton University, Ottawa, Canada [daniel@math.carleton.ca]
[3] Faculty of Mathematics and Computer Science, Amirkabir University of Technology, Tehran, Iran [msadeghi@aut.ac.ir]

Lattice coding theory is an active research area in communications. An important problem in this area is efficient lattice decoding. Label codes are crucial parameters in lattice theory, used as a template for encoding and decoding a lattice [1].

The number of codewords in a label code gives information about the trellis complexity. Finding a less complex trellis with minimum size results in a more efficient decoding algorithm [2].

In this talk, we first show a relation between the ideal of an integer lattice and its label code for any integer lattice. As an application, we obtain the reduced Gröbner bases for the root lattice D_n, and then, find a generating set for D_n's label code.

Keywords
lattice theory, label codes, Gröbner bases

References

[1] G. D. Forney, Jr., *The Viterbi algorithm.* In: *Proc. IEEE.*, **volume** 61, 268–278, 1973.

[2] V. Tarokh and I. F. Blake, *Trellis complexity versus the coding gain of lattice I.* In: *IEEE Trans. Information Theory*, **volume** 42, 1796–1807, 1996.

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *“Effective ideal theory and combinatorial techniques in commutative and non commutative rings and their applications”*

On Toric Resolutions of Rational Singularities

BÜŞRA KARADENİZ ŞEN [busrakaradeniz@gtu.edu.tr]

Mathematics Department, Gebze Technical University, Kocaeli, Turkey

Let $f \in \mathbb{C}[x,y,z]$. The vanishing set of f defines an hypersurface X in $\mathbb{C}^3$. We are interested in finding a toric resolution of X when X has singularity along one of the axes. We construct a toric resolution of X from a regular subdivision of its dual Newton polyhedron. We first study on the minimality of the resolution and then, we relate the minimal resolution with the jet space $J_m(X)$ of X which is defined as follows: Let $m \in \mathbb{N}$. The m^{th} jet of X is a parametrized curve given by

$$\varphi\colon \frac{\mathbb{C}[x,y,z]}{<f>} \to \frac{\mathbb{C}[t]}{<t^{m+1}>}$$
$$(x,y,z) \mapsto (x(t),y(t),z(t))$$

where $x(t) = x_0 + x_1 t + x_2 t^2 + \ldots + x_m t^m \pmod{t^{m+1}}$

$$y(t) = y_0 + y_1 t + y_2 t^2 + \ldots + y_m t^m \pmod{t^{m+1}}$$

$$z(t) = z_0 + z_1 t + z_2 t^2 + \ldots + z_m t^m \pmod{t^{m+1}}$$

This map gives

$$\varphi^*\colon Spec(\frac{\mathbb{C}[t]}{<t^{m+1}>}) \to Spec(\frac{\mathbb{C}[x,y,z]}{<f>})$$

We have $f(x(t),y(t),z(t)) = F_0 + tF_1 + t^2F_2 + \ldots + t^mF_m = 0 \pmod{t^{m+1}}$.

The m^{th} jet space of X is

$$J_m(X) := Spec(\frac{\mathbb{C}[x_i,y_i,z_i;\ \ i=1,\ldots m]}{<F_0,F_1,\ldots,F_m>})$$

This is a part of the joint work with C.Plénat and M.Tosun.

Keywords
Toric resolution, rational singularity, jet space.

References

[1] A. Altintas Sharland, G. Cevik, M. Tosun, *Nonisolated forms of rational triple singularities*. Rocky Mountain J. Math. 46, No.2, 357-388, 2016.
[2] B. Karadeniz, H.Mourtada, C.Plénat, M.Tosun, *The embedded Nash problem of birational models of rational triple singularities*. Journal of Singularities, Volume 22, 337-372, 2020.
[3] C. Bouvier, G. Gonzalez-Sprinberg, *Sysyéme générateur minimal, diviseurs essentiels et G-désingularisations de variétés torique*. Tohoku Math. J. 47, 125-149, 1995.

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *“Effective ideal theory and combinatorial techniques in commutative and non commutative rings and their applications”*

Sum of Disjoint Products approach to System Reliability based on Involutive Divisions

Rodrido Iglesias[1]***, Patricia Pascual-Ortigosa***[1]***,Eduardo Sáenz-de-Cabezón***[1] [esaenz-d@unirioja.es]

[1] Departamento de Matemáticas y Computación, Universidad de La Rioja, Spain

The evaluation of system reliability is an NP-hard problem even in the binary case. There exist several general methodologies to analyze and compute system reliability [6, 11]. Two main ones are the sum-of-disjoint-products (SDP), which expresses the logic function of the system as a union of disjoint terms, and the Improved Inclusion-Exclusion (IIE) formulas [4, 2]. The algebraic approach to system reliability, assigns a monomial ideal to the system and computes its reliability in terms of the Hilbert series of the ideal, providing an algebraic version of the IIE method [5, 8, 9, 7]. In this paper we make use of this monomial ideal framework and present an algebraic version of the SDP method, based on a combinatorial decomposition of the system's ideal [3, 10]. Such a decomposition is obtained from an involutive basis of the ideal. This algebraic version is suitable for binary and multi-state systems. We include computer experiments on the performance of this approach using the C++ computer algebra library CoCoALib [1] and a discussion on which of the algebraic methods can be more efficient depending on the type of system under analysis.

Keywords
Algebraic Reliability, Sum of Disjoint Products, Involutive Bases

References

[1] A. M. Bigatti, P. Pascual-Ortigosa, and E. Sáenz-de Cabezón. A c++ class for multi-state algebraic reliability computations. *Reliability Engineering and System Safety*, 213:107751, 2021.

[2] K. Dohmen. *Improved Bonferroni inequalities via abstract tubes*. Springer, 2003.

[3] Vladimir Gerdt and Yuri Blinkov. Involutive bases of polynomial ideals. *Mathematics and Computers in Simulation*, 45:519–542, 1998.

[4] B. Giglio, D. Q. Naiman, and H. P. Wynn. Gröbner bases, abstract tubes, and inclusion–exclusion reliability bounds. *IEEE Trans. Rel.*, 51:358–366, 2002.

[5] B. Giglio and H. P. Wynn. Monomial ideals and the scarf complex for coherent systems in reliability theory. *Annals of Statistics*, 32:1289–1311, 2004.

[6] W. Kuo and M Zuo. *Optimal reliability modelling: principles and applications*. John Wiley & sons, 2003.

[7] F. Mohammadi, P. Pascual-Ortigosa, E. Sáenz-de-Cabezón, and H.P. Wynn. Polarization and depolarization of monomial ideals with application to multi-state system reliability. *Journal of Algebraic Combinatorics*, 51:617–639, 2020.

[8] E. Sáenz-de-Cabezón and H. P. Wynn. Betti numbers and minimal free resolutions for multi-state system reliability bounds. *Journal of Symbolic Computation*, 44:1311–1325, 2009.

[9] E. Sáenz-de-Cabezón and H. P. Wynn. Hilbert functions for design in reliability. *IEEE Trans. Rel.*, 64:83–93, 2015.

[10] Werner M. Seiler. *Involution*. Springer Verlag, 1st edition, 2010.

[11] K.S. Trivedi and A. Bobbio. *Reliability and availability engineering*. Cambridge University Press, 2017.

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15–19, 2022
Session on *"Algorithmic & Experimental Combinatorics"*

Searching for Kochen–Specker systems with orderly generation and satisfiability solving

Curtis Bright[1]***, Zhengyu Li***[2]***, Vijay Ganesh***[3]

[1] School of Computer Science, University of Windsor, Windsor, Canada
[2] Department of Mathematical and Computational Sciences, University of Toronto, Mississauga, Canada
[3] Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Canada

There are a number of ways of generating combinatorial objects "up to isomorphism" [6]. An approach often used in the symbolic computation community is to iteratively construct objects using an isomorph-free method such as orderly generation [4, 7]. Alternatively, the satisfiability (SAT) community often removes isomorphic solutions from the search via the addition of new constraints [2]. Coupling isomorph-free exhaustive generation with satisfiability checking has been explored recently [1,5,8].

We use orderly generation and SAT solving to search for Kochen–Specker (KS) systems—a crucial ingredient used in the proof of the "Free Will Theorem" that if humans have free will then so do elementary particles [3]. We show that augmenting a SAT solver with orderly generation dramatically improves its performance, especially as the size of the search increases. Our search for KS systems of size 21 is over a thousand times faster than the previous best approach [9] and we derive a new lower bound by showing a KS system must be of size 23 or greater.

Keywords
Isomorph-free exhaustive generation, orderly generation, satisfiability solving, symbolic computation, symmetry breaking, search, Kochen–Specker systems

References

[1] C. Bright; K. K. H. Cheung; B. Stevens; I. Kotsireas; V. Ganesh. A SAT-based resolution of Lam's problem. In *Proceedings of the Thirty-Fifth AAAI Conference on Artificial Intelligence*, pages 3669–3676, 2021.
[2] M. Codish; A. Miller; P. Prosser; P. J. Stuckey. Constraints for symmetry breaking in graph representation. *Constraints*, **24**(1):1–24, 2019.
[3] J. Conway; S. Kochen. The free will theorem. *Foundations of Physics*, **36**(10):1441–1473, 2006.
[4] I. A. Faradžev. Constructive enumeration of combinatorial objects. In *Problèmes combinatoires et théorie des graphes*, pages 131–135, 1978.

[5] T. JUNTTILA; M. KARPPA; P. KASKI; J. KOHONEN. An adaptive prefix assignment technique for symmetry reduction. *Journal of Symbolic Computation*, **99**:21–49, 2020.

[6] P. KASKI; P. R. J. ÖSTERGÅRD. Classification Algorithms for Codes and Designs. Springer-Verlag, 2006.

[7] R. C. READ. Every one a winner or how to avoid isomorphism search when cataloguing combinatorial configurations. *Annals of Discrete Mathematics*, **2**:107–120, 1978.

[8] J. SAVELA; E. OIKARINEN; M. JÄRVISALO. Finding periodic apartments via Boolean satisfiability and orderly generation. In *Proceedings of the 23rd International Conference on Logic for Programming, Artificial Intelligence and Reasoning*, pages 465–482, 2020.

[9] S. UIJLEN; B. WESTERBAAN. A Kochen-Specker system has at least 22 vectors. *New Generation Computing*, **34**(1-2):3–23, 2016.

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *"Algorithmic & Experimental Combinatorics"*

Counting points of modular curves over finite fields

Valerio Dose*[1], *Pietro Mercuri*[2], *Claudio Stirpe [mercuri.ptr@gmail.com]

[1] Department of Computer, Control and Managing Engineering (DIAG), "Sapienza" Università di Roma, Rome, Italy,
[2] SBAI Department, "Sapienza" Università di Roma, Rome, Italy,
[3] Convitto Nazionale R. Margherita, Anagni, Italy

At the intersection of algebraic geometry, number theory, and combinatorics (especially in finite geometry), an interesting problem is counting points on an algebraic curve over a finite field. For an elliptic curve E over a finite field $\mathbb{F}_q$, with q a prime power, it is classically well known that $\#E(\mathbb{F}_q) = 1 + q - a_q$, where the a_q's are the eigenvalues of suitable (Hecke) operators acting on E. This can be generalized to modular curves (that are curves parametrizing elliptic curves with some torsion data). If we know the eigenvalues of Hecke operators, we can compute the number of points of a modular curve over finite fields very quickly. Algorithms for computing eigenvalues of Hecke operators allowed us to make these calculations for a very large number of examples. This data gives us a large amount of experimental information that we can study, in particular, we are interested in curves with many points over finite fields with respect to the genus (these kinds of curves are interesting for applications to codes).

Keywords
Modular Curves, Finite Fields

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *“Algorithmic & Experimental Combinatorics”*

Experimenting with Young Tableaux

Dron Zeilberger[1] [doronzeil@gmail.com]

[1] Rutgers University, New Jersey, United States of America

Young tableaux are simple to define, easy to count, yet there are still lots of fascinating open problems. They can also be explored by simulation, using the seminal Greene-Nijenhuis-Wilf algorithm to generate, uniformly at random, a standard Young tableau of a given shape.

Keywords
Young Tableaux, Greene-Nijenhuis-Wilf algorithm

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *“Algorithmic & Experimental Combinatorics”*

Schmidt type partitions

Ae Ja Yee[1] [yee@psu.edu]

[1] Pennsylvania State University, College Park, United States of America

Recently, Andrews and Paule studied Schmidt type partitions using MacMahon’s Partition Analysis and obtained various interesting results. In this talk, I will discuss the combinatorics of the Schmidt type partition theorems of Andrews and Paule along with some generalizations and overpartition analogues.

Keywords
Schmidt type partitions, Overpartitions

Applications of Computer Algebra – ACA 2022
Istanbul-Gebze, Turkey | August 8-26, 2022
Session on *"Algorithmic & Experimental Combinatorics"*

The Factorial-Basis Method for Finding Definite-Sum Solutions of Linear Recurrences

Antonio Jiménez-Pastor[1] [jimenezpastor@lix.polytechnique.fr]

[1] LIX, CNRS, École Polytechnique, Institute Polytechnique de Paris, Palaiseau, France

In this talk we will describe the Factorial-Basis method and its current implementation in SageMath [7] to obtain definite-sum solutions for linear recurrences.

By definition, a *P-recursive* (or *holonomic*) sequence is given by a linear recurrence with polynomial coefficients, together with suitable initial conditions. Often one wishes to find *explicit representations* of P-recursive sequences and plenty of algorithms has been developed to find solutions of specific shape. For example, one can find polynomial [1], rational [2], hypergeometric [6], D'Alembertian [3] or Liouvillian [4] solutions.

However, these classes do not exhaust all possible representable P-recursive sequence. For instance, every definite hypergeometric sum on which Zeilberger's Creative Telescoping algorithm [8] succeeds. Hence, it makes sense to consider the *Inverse Creating Telescoping Problem*:

Problem. Given a linear recurrence $\mathcal{L}$ with polynomial coefficients and no Liouvillian solutions, find its solution in the form of *definite sums* of a given type.

In this talk we present a small, but important, step towards solving this problem: given a linear recurrence $\mathcal{L}$ with polynomial coefficients and a polynomial basis (i.e., a set $\mathcal{B} = \{P_n(x) \mid n \in \mathbb{N}\}$ with $\deg(P_n(x)) = n$) that is *shift-compatible* and *quasi-triangular*, we compute another recurrence $\mathcal{L}'$ such that if

$$y = \sum_{k=0}^{\infty} c_k P_k(n),$$

then $\mathcal{L}y = 0$ if and only if $\mathcal{L}'c = 0$. Hence, we can transform recurrence operators into simpler ones that we can solve with existing algorithms. With appropriate iteration, one can, in the end, express the original sequence y as a definite-sum of simpler sequences.

Example. Consider the simple linear operator $\mathcal{L} = E - c$ where E is the shift mapping $x \mapsto x + 1$ and $c \in \mathbb{K}$. If we look the equation $\mathcal{L}y(x) = 0$ with $x \in \mathbb{N}$, we know we have the solution $y(m) = \alpha c^m$ for any $\alpha \in \mathbb{K}$.

Now, consider the binomial basis $\mathcal{C} = \left\{\binom{x}{n} \mid n \in \mathbb{N}\right\}$ and $y(x) = \sum_{n\geq 0} a_n\binom{x}{n}$. Using the well known identity $\binom{x+1}{n} = \binom{x}{n} + \binom{x}{n-1}$, we have that $\mathcal{L}y = 0$ if and only if

$$\sum_{n\geq 0}(a_{n+1} - (c-1)a_n)\binom{x}{n} = 0,$$

which means that the sequence (a_n) satisfies the recurrence $a_{n+1} - (c-1)a_n = 0$. This recurrence has as solution $a_n = \alpha(c-1)^n$. Hence, putting everything together, we obtain a new representation for the sequence $(c^n)_n$ with a well-known binomial identity:

$$c^m = \sum_{n=0}^{m}(c-1)^n\binom{m}{n}.$$

□

This toy example, although simple itself, shows already the key theoretical concept that allows us to understand and automatize all these ideas: the *compatibility* of linear operators with polynomial basis.

Definition. Let $\mathcal{L}$ be a linear operator over $\mathbb{K}[x]$ and $\mathcal{B} = \{P_n(x) \mid n \in \mathbb{N}\}$ a polynomial basis such that $\deg(P_n(x)) = n$. We say that $\mathcal{L}$ is compatible with $\mathcal{B}$ if there are $A, B \in \mathbb{N}$ and coefficients $\alpha_i(n)$ for $i = -A, \ldots, B$ such that, for all $n \in \mathbb{N}$:

$$\mathcal{L}P_n(x) = \sum_{i=-A}^{B} \alpha_i(n)P_{n+i}(x).$$

Given a particular polynomial basis $\mathcal{B}$, the set of compatible operators form a $\mathbb{K}$-algebra, and computing the exact compatibility coefficients $\alpha_i(n)$ is a straightforward computation. From this point on we focus on a special type of polynomial bases: factorial bases. These basis satisfy a recurrence of order one, i.e., for all $n \in \mathbb{N}$:

$$P_{n+1}(x) = (a_n x + b_n)P_n(x).$$

We then proceed combine these factorial basis obtaining more complex factorial bases in order to obtain basis that contains some products of binomial coefficients of appropriate shape. We can do this using the concepts of *Product basis* and *Shuffled bases*. These two similar ways of mixing factorial bases produce new factorial bases in such a way that, if the original bases were compatible with an operator $\mathcal{L}$, then the new basis is again compatible with $\mathcal{L}$.

We will present all this concepts and their implementation in SageMath [7] within the package `pseries_basis`. This package is freely available on Github[*].

This talk is a joint work with M. Petkovšek and based on the article [5].

Keywords
hypergeometric sums, (formal) polynomial series; quasi-triangular bases; p-recursive; holonomic

[*] https://www.github.com/Antonio-JP/pseries_basis

References

[1] S.A. Abramov, Problems in computer algebra that are connected with a search for polynomial solutions of linear differential and difference equations. *Moscow Univ. Comput. Math. Cybernet* **3**, 63–68 (1989).

[2] S.A. Abramov, Rational solutions of linear difference and q-differenceequations with polynomial coefficients. *Programming and Comput. Software* **21**, 273–278 (1995).

[3] S.A. Abramov, M. Petkovšek, D'Alembertian solutions of linear operator equations. In *Proceeding ISSAC'94*, 169–174. Oxford (1994)

[4] P.A. Hendriks, M. Singer, Solving difference equations in finite terms. *J. Symbolic Comput.* **27**, 109–131 (1999).

[5] A. Jiménez-Pastor, M. Petkovšek, The Factorial-Basis Method for Finding Definite-Sum Solutions of Linear Recurrences With Polynomial Coefficients. *ArXiv* **arXiv:2202.05550** (2022).

[6] M. Petkovšek, Hypergeometric solutions of linear recurrences with polynomial coefficients. *J. Symbolic Comput.* **14**, 243–264 (1992).

[7] the Sage Developers, *SageMath, the Sage Mathematics Software System (Version 9.5)*(2021), `https://www.sagemath.org`

[8] D. Zeilberger, The method of creative telescoping. *J. Symbolic Comput.* **11**, 195–204 (1991).

Applications of Computer Algebra – ACA 2022
August 15–19, 2022
Session on *"Algorithmic & Experimental Combinatorics"*

Regular languages and the enumeration of permutation classes

Vincent Vatter[1] [vatter@ufl.edu]

[1] Department of Mathematics, University of Florida, Gainesville, Florida, USA

Attempts to apply the mature theory of regular languages to the study of permutation patterns date to the 2003 work of Albert, Atkinson, and Ruškuc [2], who essentially reinvented the *Lehmer code*. Albert, Linton, and Ruškuc [3] later generalized this approach to create the *insertion encoding*. This encoding is well understood: we have a theorem characterizing precisely which permutation classes it can handle, and Vatter [4] shows how to implement the encoding in practice while avoiding much of the NDFA-to-DFA blow-up one might otherwise expect. Somewhat independently, Albert, Atkinson, Bouvel, Ruškuc, and Vatter [1] have introduced *geometric grid classes* of permutations, and have proved that they are in bijection with regular languages. In contrast to the situation with the insertion encoding, here we know frustratingly little about the encoding: we have no algorithm to determine whether it applies to a given permutation class (described by a finite list of avoided permutations), and the proof of the regularity of the languages is entirely non-constructive, as it rests in an essential way on Higman's lemma. I will describe efforts to make these results constructive and implementable.

Keywords
enumeration, regular languages, permutation patterns

References

[1] M. ALBERT; M. ATKINSON; M. BOUVEL; N. RUŠKUC; V. VATTER, Geometric grid classes of permutations. *Trans. Amer. Math. Soc.* **365**(11), 5859–5881 (2013).
[2] M. ALBERT; M. ATKINSON; N. RUŠKUC, Regular closed sets of permutations. *Theoret. Comput. Sci.* **306**(1-3), 85–100 (2003).
[3] M. ALBERT; S. LINTON; N. RUŠKUC, The insertion encoding of permutations. *Electron. J. Combin.* **12**(1), Paper 47, 31 pp. (2005).
[4] V. VATTER, Finding regular insertion encodings for permutation classes. *J. Symb. Comput.* **47**(3), 259–265 (2012).

Applications of Computer Algebra – ACA 2022
Virtual. Online | August 15-19, 2022
Session on *“Algorithmic and Experimental Combinatorics”*

Well-Indumatched Pseudoforests

Yasemin Büyükçolak[1]***, Didem Gözüpek***[2]***, Sibel Özkan***[1] [y.buyukcolak@gtu.edu.tr]

[1] Mathematics Department, Gebze Technical University, Kocaeli, Turkey
[2] Computer Engineering Department, Gebze Technical University, Kocaeli, Turkey

A *matching* in a graph G is a set of nonadjacent edges in the edge set of G. An *induced matching* in a graph G is a matching such that no two end vertices of two different edges in the matching are joined by an edge. A graph G is *well-indumatched* if all its maximal induced matchings have the same size, that is, every maximal induced matching in G has the same cardinality. The well-indumatched graphs were introduced in 2017 by Baptiste et al. [1]. They proved that recognizing a well-indumatched graph is a co-NP-complete problem even for $(2P_5, K_{1,5})$-free graphs. More recently, Akbari et al. [2] provided a characterization of well-indumatched acyclic graphs and this characterization yields a linear time recognition algorithm. The authors also showed that there are infinitely many well-indumatched unicyclic graphs of girth k, where $k \in \{3, 5, 7\}$ or k is an even integer greater than 2 by providing the well-indumatched graph families.

In this work, we provide a complete structural characterization of well-indumatched pseudotrees, which are well-indumatched graphs whose each connected component contains at most one cycle. That is, well-indumatched pseudotrees are disjoint union of well-indumatched trees and well-indumatched unicyclic graphs. We define the *pseudotree decomposition* of a well-indumatched unicyclic graph as pseudotrees, which contain at least two components where only one of which is a well-indumatched unicyclic graph and all other components are well-indumatched trees. Using the characterization of well-indumatched trees in [2] and pseudotree decomposition, we extend the results on well-indumatched unicyclic graphs in [2] by identifying all well-indumatched unicyclic graph families.

Keywords
Induced Matching, Well-Indumatched Graphs, Pseudotrees, Unicyclic Graphs

References

[1] P. BAPTISTE, M.Y. KOVALYOV, Y.L. ORLOVICH, F. WERNER AND I.E. ZVEROVICH, Graphs with maximal induced matchings of the same size. *Discrete Applied Mathematics* **216**, 15–28 (2017).
[2] S. AKBARI, T. EKIM, A.H. GHODRATI AND S. ZARE, Well-indumatched Trees and Graphs of Bounded Girth. arXiv:1903.03197, preprint.

Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *“Algoritmic and Experimental Combinatorics”*

Counting Labelled Trees of Certain Families

Emre Yivli[1,2]***, Emrah Akyar***[1]***, Handan Akyar***[1] [eyivli@nku.edu.tr]

[1] Mathematics Department, Eskisehir Technical University, Eskisehir, Turkey
[2] Mathematics Department, Tekirdag Namik Kemal University, Tekirdag, Turkey

A tree with n vertices is called a labelled tree if its vertices are distinguished from one another by names such as, $l_1, l_2, \ldots, l_n$. Even if two trees are isomorphic, trees with having different vertex labels are considered as distinct graphs. According to Cayley's tree formula [1], there are n^{n-2} labelled trees on n vertices. Prüfer used a simple way to prove this formula and demonstrated that there exists a bijection between the set of labelled trees on n vertices and sequences of $n-2$ numbers, each in the range $0, 1, 2, \ldots, n-1$ [2]. Such a number sequence is called a Prüfer code and it provides an alternative to the usual representation of trees.

In this study, a computer algebra system (Maple) [3] library containing various algorithms for trees is presented with the help of Prüfer code. Moreover, the number of labelled trees for various families of trees such as double star, spider, centipede, firecracker, etc. is calculated using combinatorial methods with the help of Prüfer code.

Keywords
Labelled Tree, Prüfer Code, Computer Algebra System

References

[1] Cayley A., A Theorem on Trees. *Q. J. Math.* **23**, 376–378 (1889).
[2] Prüfer, H., Neuer Beweis eines Satres über Permutationen. *Arch. Math. Phys.* **27**, 742–744 (1918).
[3] Maple (2019). Maplesoft, a division of Waterloo Maple Inc., Waterloo, Ontario.

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey,| August 15-19, 2022
Session on *"Algorithmic and Experimental Combinatorics"*

On the Directed Hamilton-Waterloo Problem with Uniform Cycle Sizes

Fatih Yetgin[1]***, Uğur Odabaşı***[2]***, Sibel Özkan***[1] [fyetgin@gtu.edu.tr]

[1] Department of Mathematics, Gebze Technical University, Kocaeli, Turkey
[2] Department of Engineering Sciences, Istanbul University-Cerrahpasa, Istanbul, Turkey

A decomposition of a graph is a partition of its edge set into subsets. Graph decomposition is one of the central fields of study in the intersection of Graph Theory and Combinatorial Design Theory, with many applications in many other fields. Most graph decomposition problems are related to cycle decompositions.

Cycle Decomposition problems, in general, are NP-complete. Cycle factorization is a particular case of the cycle decomposition problem with additional constraints such that the decomposition can be partitioned into parallel classes which we call 2-factors. When we add the condition that the edges must be directed, the problem becomes more difficult.

There are two well-known cycle factorization problems. One problem is the Oberwolfach Problem where K_v (or $K_v - I$) decomposes into isomorphic 2-factors. Another problem is the Hamilton-Waterloo Problem where K_v (or $K_v - I$) decomposes into 2-factors, and each 2-factor can be isomorphic to one of the given two 2-factors. There are numerous studies in the literature based on the uniform versions of both problems.

The Directed Hamilton-Waterloo problem requires directed cycle factorization of the complete symmetric digraph K_v^* into two non-isomorphic factors of directed cycles. If each factor consists of either directed m-cycles or n-cycles, this version of the problem is called the uniform version and is denoted by HWP$^*(v; m^r, n^s)$ where r and s are the number of factors of directed m-cycles and n-cycles such that $r + s = v - 1$, respectively. In this study, the necessary conditions for a solution to HWP$^*(v; m^r, n^s)$ are given. Also some solutions to the uniform version of the Directed Hamilton-Waterloo Problem depending on the parity of the cycle sizes are presented.

Keywords
The Directed Hamilton-Waterloo Problem, cycle decomposition, directed factorization, complete symmetric digraph, directed cycle

References

[1]B. Alspach, H. Gavlas, M. Sajna, and H. Verrall, Cycle decompositions IV: complete directed graphs and fixed length directed cycles, *J. Comb. Theory Ser. A.* **103**(1),

165-208 (2003).

[2] P. Adams, E. J. Billington, D. E. Bryant, and S. I. El-Zanati, On the Hamilton-Waterloo problem, *Graphs Combin.* **18**, 31-51 (2002).

[3] D. Bryant, P. Danziger, On bipartite 2-factorizations of $K_n - I$ and the Oberwolfach problem, *J. Graph Theory* **68**(1), 22-37 (2011).

[4]D. Bryant, P. Danziger, and M. Dean, On the Hamilton-Waterloo Problem for Bipartite 2-Factors, *J. Comb. Des.* **21**(2), 60-80 (2013).

[5] J. C. Bermond, A. Germa, and D. Sotteau, Resolvable decomposition of K_n^*, *J. Comb. Theory Ser. A.* **26**(2), 179-185 (1979).

[6] F. E. Bennett, X. Zhang, Resolvable Mendelsohn designs with block size 4, *Aequationes Math.* **40**(1), 248-260 (1990).

[7] A. Burgess, N. Francetic, and M. Sajna, On the directed Oberwolfach Problem with equal cycle lengths: the odd case, *Australas. J. Comb.* **71**(2), 272-292 (2018).

[8] A. Burgess, M. Sajna, On the directed Oberwolfach Problem with equal cycle lengths, *Electron. J. Comb.* **21**(1), 1-15 (2014).

[9] A. Burgess, P. Danziger, and T. Traetta, On the Hamilton-Waterloo problem with odd orders, *J. Comb. Des.* **25**(6), 258-287 (2017).

[10] A. Burgess, P. Danziger, and T. Traetta, On the Hamilton-Waterloo problem with odd cycle lengths, *J. Comb. Des.* **26**(2), 51-83 (2018).

[11] S. Bonvicini, M. Buratti, Octahedral, dicyclic and special linear solutions of some Hamilton-Waterloo problems, *Ars Math. Contemp.* **14**(1), 1-14 (2017).

[12] P. Danziger, G. Quattrocchi, and B. Stevens, The Hamilton-Waterloo problem for cycle sizes 3 and 4, *J. Comb. Des.*, **17**(4), 342-352 (2009).

[13] R. K. Guy, *Unsolved combinatorial problems, In: Proceedings of the Conference on Combinatorial Mathematics and Its Applications*, Oxford, 1967 (D. J. A. Welsh, Ed.), Academic Press, New York, 1971.

[14] R. Haggkvist, A lemma on cycle decompositions, North-Holland Mathematics Studies **115**, 227-232 (1985).

[15] W. Imrich, S. Klavzar, *Product graphs: Structure and Recognition*, John Wiley and Sons Incorporated, New York, 2000.

[16] M. Keranen, S. Özkan, The Hamilton-Waterloo problem with 4-cycles and a single factor of n-cycles, *Graphs Combin.* **29** , 1827–1837 (2013).

[17] J. Liu, The equipartite Oberwolfach problem with uniform tables, *J. Comb. Theory Ser. A.* **101**, 20–34 (2003).

[18] E. Shabani, M. Sajna, On the Directed Oberwolfach Problem with variable cycle lengths, 2020, arXiv preprint arXiv:2009.08731.

[19] U. Odabaşı, S. Özkan, The Hamilton-Waterloo problem with C_4 and C_m factors, *Discrete Math.* **339**(1), 263-269 (2016).

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *“Algorithmic & Experimental Combinatorics”*

On generalizations of the third order mock theta functions $\omega(q)$ and $\nu(q)$

Atul Dixit[1], ***Bruce Berndt***[2], ***Rajat Gupta***[1] [adixit@iitgn.ac.in]

[1] IIT Gandhinagar, Palaj, India
[2] University of Illinois at Urbana–Champaign, Urbana, United States of America

George Andrews and Ae Ja Yee recently established beautiful results involving bivariate generalizations of the third order mock theta functions $\omega(q)$ and $\nu(q)$, thereby extending their earlier results with the speaker. Generalizing the Andrews-Yee identities for trivariate generalizations of these mock theta functions remained a mystery, as pointed out by Li and Yang in their recent work. We have partially solved this problem and have generalized the Andrews-Yee identities. Several new as well as well-known results have been derived. For example, one of our two main theorems gives, as a corollary, a special case of Soon-Yi Kang's three-variable reciprocity theorem. A relation between a new restricted overpartition function $p^*(n)$ and a weighted partition function $p_*(n)$ has also been obtained from a special case of one of our theorems. I will present these results and also put forth some challenging problems which would be interesting to pursue further.

Keywords
Mock theta functions, Overpartitions

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2021
Session on *"Algorithmic and Experimental Combinatorics"*

Linked partition ideals and computer algebra

Shane Chern[1] [chenxiaohang92@gmail.com; xh375529@dal.ca]

[1] Department of Mathematics and Statistics, Dalhousie University, Halifax, NS, B3H 4R2, Canada

The framework of linked partition ideals, which serves as an important tool for integer partition identities, was introduced by George Andrews in the 1970s. One main object of this framework concerns the construction of Andrews–Gordon type generating functions for partition sets under certain difference conditions. Briefly speaking, one may separate such partition sets into a finite number of subclasses according to their linked partition ideal decompositions. Meanwhile, the generating functions for these subclasses satisfy a certain system of q-difference equations.

Although the theory of linked partition ideals is still in its infancy after almost fifty years, it is clear that modern computer algebra systems are stimulating the development of this theory to a great extent. In this talk, I will discuss how an algorithmic procedure, which relies on matrix transformations, works in the study of the aforementioned q-difference systems. Also, I will present several instances of making use of *Mathematica* packages implemented by RISC in the construction of Andrews–Gordon type generating functions for these partition sets.

This talk contains my joint work with George Andrews and Zhitai Li [1,2].

Keywords
Linked partition ideals, Andrews–Gordon type series, Generating function, Kanade–Russell conjectures, Schur's theorem, Computer algebra

References

[1] G. E. ANDREWS; S. CHERN; Z. LI, Linked partition ideals and the Alladi–Schur theorem. *J. Combin. Theory Ser. A* **189**, Paper No. 105614, 19 pp. (2022).
[2] S. CHERN; Z. LI, Linked partition ideals and Kanade–Russell conjectures. *Discrete Math.* **343**(7), Paper No. 111876, 24 pp. (2020).

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on"Algorithmic & Experimental Combinatorics"

Missing cases in parity considerations in Rogers–Ramanujan–Gordon type overpartitions

Kağan Kurşungöz[1]**, *Mohammad Zadeh Dabbagh***[1] `[mzadehdabbagh@sabanciuniv.edu]`

[1] Faculty of Engineering and Natural Sciences, Sabanci university, Istanbul, Turkey

In 2010, Andrews imposed parity restrictions on Rogers, Ramanujan and Gordon identities. In the conclusion of the paper, he offered considering parity conditions for some overpartition identities as an open problem. In 2013, Chen, Sang and Shi proved the Rogers-Ramanujan-Gordon's identity for overpartitions. Later, in 2020, Sang, Shi and Yee put parity restriction for that identity and proved it for some cases. We followed their work and in a constructive method, developed by Kurşungöz, we re-proved their identities and proved the remaining cases.

Keywords
Partition Identity, Overpartition, Parity

References

[1] ANDREWS, G.E., *The Theory of Partitions*. The Encyclopedia of Mathematics and Its Applications Series. Addison-Wesley, New York, 1976.
[2] ANDREWS, G.E., Parity in partition identities. *Ramanujan J* (23), 45-90 (2010).
[3] DORIS D.M. SANG, DIANE Y.H. SHI, AE JA YEE, Parity considerations in Rogers–Ramanujan–Gordon type overpartitions. *Journal of Number Theory* (215), 297-320 (2020).
[4] KURŞUNGÖZ, K., Andrews style partition identities. *Ramanujan J* (36), 249–265 (2015).
[5] KURŞUNGÖZ, K., Bressoud style identities for regular partitions and overpartitions. *Journal of Number Theory* (168), 45-63 (2013).
[6] W. CHEN, D.D. SANG, D.Y. SHI,, The Rogers-Ramanujan-Gordon theorem for overpartitions. *Proc. Lond. Math. Soc.* (106), 1371-1393 (2013).

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *"Algorithmic & Experimental Combinatorics"*

The Combinatorial Exploration Framework and its Consequences

***Michael Albert*[1], *Christian Bean*[2], *Anders Claesson*[3], *Émile Nadeau*[2], *Jay Pantone*[4], *Henning Ulfarsson*[2]** `[henningu@ru.is]`

[1] Department of Computer Science, University of Otago, New Zealand
[2] Department of Computer Science, Reykjavik University, Iceland
[3] Division of Mathematics, The Science Institute, University of Iceland, Iceland
[4] Department of Mathematical and Statistical Sciences, Marquette University, USA

In the article [1] we introduced *Combinatorial Exploration* as a framework to algorithmically discover the structure of combinatorial classes. When the exploration is successful a combinatorial specification of the initial class is output. Although the framework is domain agnostic we have focused on the study of permutation classes. We have successfully reproduced in a unified manner results in the literature spanning dozens of articles, as well as finding new statements.[*] With one of our specifications in hand we always produce a polynomial time algorithm to enumerate the elements (by length) in the class, as well as a system of equations, sometimes in several variables. In many cases we can solve these systems of equations to obtain a generating function for the enumeration. Furthermore we can often use the specification to generate large permutations uniformly at random. This allows us to create *heatmaps* of classes, by overlaying several random permutations on top of each other. We will survey our results and discuss future directions. For examples of specifications, heatmaps, and obtaining a copy of our implementation, please refer to the website `https://permpal.com`.

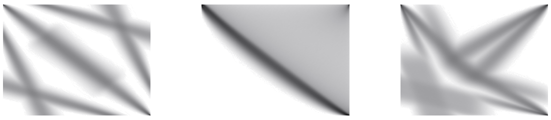


Figure 1: Heatmaps of three permutation classes

Keywords
Permutation patterns, algorithmic enumeration, combinatorial specification

[*] In particular we have been able to find combinatorial specifications for 6 out of the 7 principal classes of length 4, and every other class defined by the avoidance of two or more length 4 patterns. See section 2.4 in our paper for a comprehensive list with references.

References

[1] M. Albert, C. Bean, A. Claesson, É. Nadeau, J. Pantone, and H. Ulfarsson, Combinatorial Exploration: An algorithmic framework for enumeration. https://arxiv.org/abs/2202.07715 (2022).

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *"Algorithmic & Experimental Combinatorics"*

Partitions, Kernels, and the Localization Method

Nicolas Smoot[1] [nsmoot@risc.jku.at]

[1] Research Institute for Symbolic Computation, Johannes Kepler University, Linz, Austria

We provide some recent results in the arithmetic properties of the k-elongated plane partition function. In particular, we discuss infinite congruence families for $d_k(n)$ which have been found modulo powers of 2, 3, and 5, with possibilities for 7 and 11. These results have stemmed from the application of new techniques for proving partition congruence families, which reveal an unexpected internal algebraic structure within rational polynomials in a given Hauptmodul.

Keywords
Localization method, Partition congruences

Applications of Computer Algebra – ACA 2022
Gebze Technical University | August 15-19, 2022
Session on *“Algorithmic and Experimental Combinatorics”*

Combinatorial constructions of generating functions of cylindric partitions with small profiles into unrestricted or distinct parts

Kağan Kurşungöz[1], ***Halime Ömrüuzun Seyrek***[1]

[halimeomruuzun@alumni.sabanciuniv.edu]

[1] Mathematics Department, Sabanci University, İstanbul, Turkey

Cylindric partitions into profiles $c = (1, 1)$ and $c = (2, 0)$ are considered. The generating functions into unrestricted cylindric partitions and cylindric partitions into distinct parts with these profiles are constructed. The constructions are combinatorial and they connect the cylindric partitions with ordinary partitions. The generating function of cylindric partitions with the said profiles turn out to be combinations of two infinite products.

Keywords
integer partitions, cylindric partitions, partition generating function

References

[1] G. E. ANDREWS, An analytic generalization of the Rogers-Ramanujan identities for odd moduli. *Proceedings of the National Academy of Sciences* **71** (10), 4082–4085 (1974).
[2] G. E. ANDREWS, *The theory of partitions*. No. 2. Cambridge university press, 1998.
[3] A. BORODIN, Periodic Schur process and cylindric partitions. *Duke Math. J.* **140** (3), 391–468 (2007).
[4] S. CORTEEL, J. DOUSSE AND A.K. UNCU, Cylindric partitions and some new Rogers–Ramanujan identities. *Proc. Amer. Math. Soc.* **150** (2022), 481–497 (2021).

[5] S. Corteel and T. Welsh, The A_2 Rogers–Ramanujan Identities Revisited. *Ann. Comb.* **23** 683–694 (2019).

[6] O. Foda and T.A. Welsh, Cylindric partitions, $\mathcal{W}_r$ characters and the Andrews–Gordon–Bressoud identities. *Journal of Physics A: Mathematical and Theoretical* **49** (16) 164004 (2016).

[7] I.M. Gessel and C. Krattenthaler, Cylindric partitions. *Trans. Amer. Math. Soc.* **349** (2) 429–479 (1997).

[8] A. Iqbal, C. Kozçaz and K. Shabbir, Refined topological vertex, cylindric partitions and U(1) adjoint theory. *Nuclear Physics B* **838** (3) 422–457 (2010).

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *"Algorithmic & Experimental Combinatorics"*

Sum-of-tails Identities

Rajat Gupta[1] [rajatgpt@gate.sinica.edu.tw]

[1] Institute of Mathematics, Academia Sinica, Taiwan

In this talk, a

finite analogue of the generalized sum-of-tails identity of Andrews and Freitas is obtained. We derive several interesting results as special cases of this analogue, in particular, a recent identity of Dixit, Eyyunni, Maji and Sood. We derive a new extension of Abel's lemma with the help of which we obtain a one-parameter generalization of a sum-of-tails identity of Andrews, Garvan and Liang, an identity of Ramanujan as well as two new results —one for Ramanujan's function $\sigma(q)$ and another for the function recently introduced by Andrews and Ballantine. Later we introduce a new generalization $FFW_c(n)$ of a function of Fokkink, Fokkink and Wang and derive an identity for its generating function. This gives, as a special case, a recent representation for the generating function of $spt(n)$ given by Andrews, Garvan and Liang. We also obtain some weighted partition identities along with new representations for two of Ramanujan's third order mock theta functions through combinatorial techniques.

Keywords
Sum-of-tails, SPT function, Mock theta functions

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2021
Session on *"Algorithmic and Experimental Combinatorics"*

Efficient Rational Creative Telescoping

Mark Giesbrecht[1], ***Hui Huang***[2], ***George Labahn***[1], ***Eugene Zima***[3] [huanghui@dlut.edu.cn]

[1] Cheriton School of Computer Science, University of Waterloo, Waterloo, Canada
[2] School of Mathematical Sciences, Dalian University of Technology, Dalian, China
[3] Physics and Computer Science, Wilfrid Laurier University, Waterloo, Canada

We present a new algorithm to compute minimal telescopers for rational functions in two discrete variables. As with recent reduction-based approaches, our algorithm has the important feature that the computation of a telescoper is independent of its certificate. In addition, our algorithm uses a compact representation of the certificate, which allows it to be easily manipulated and analyzed without knowing the precise expanded form. This representation hides potential expression swell until the final (and optional) expansion, which can be accomplished in time polynomial in the size of the expanded certificate. A complexity analysis, along with a Maple implementation, indicates that our algorithm has better theoretical and practical performance than the reduction-based approach in the rational case.

Keywords
Rational function, GGSZ reduction, Left scalar division with remainder, Telescoper

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2021
Session on *"Session Title"*

A Gessel Way to the Diagonal Theorem on D-finite Power Series

Shaoshi Chen[1]***, Pingchuan Ma***[1]***, and Chaochao Zhu***[2] [schen@amss.ac.cn]

[1] KLMM, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing, 100190, China
[2] College of Finance and Mathematics, West Anhui University, Luan, Anhui, 237012, China

Special functions that satisfy linear differential equations with polynomial coefficients appear ubiquitously in combinatorics and mathematical physics. Such kind of special functions are called D-finite functions by Stanley. In the early 1980's, many combinatorists, such as Gessel, Stanley, Zeilberger etc., conjectured that the diagonal of rational power series in several variables is D-finite. Gessel and Zeilberger proved this conjecture in their papers, respectively. Later, Lipshitz pointed out that their proofs are not complete and he gave a proof by basing on a different idea. Zeilberger completed his proof with the theory of holonomic D-modules. In this talk, we follow the spirit of Gessel's proof strategy and fix the gap in his proof. The key ingredients we used are some basic properties of the diagonal operation. This is a joint work with Pingchuan Ma and Chaochao Zhu.

Keywords
D-finite power series, Diagonal theorem

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *"Algorithmic & Experimental Combinatorics"*

Factorizable systems of differential equations from particle physics: preprocessing and solving

Nikolai Fadeev[1] [j.smith@ulb.be]

[1] Research Institute for Symbolic Computation, Johannes Kepler University, Linz, Austria

While solving systems of linear differential equations in one variable is straightforward when the coefficients are constant, in the case when those coefficients depend on several variables, the problem becomes more challenging. For example, in particle physics, computing Feynman integrals can be done using the "integration by parts" method where we have to solve an inhomogeneous first order differential system that depends also on a (regularisation) parameter epsilon. There exist several methods that allow one to solve this system order by order in epsilon, either using the differential equation setting, the difference field and ring machinery, or the large moment method. Most of those strategies rely on an efficient preprocessing of the system that provides the best uncoupling order and associated linear differential equations to solve. Special care has to be done to find an uncoupling such that the underlying expansion in epsilon is optimized. After introducing the general problem and briefly presenting the different methods, we will present a new preprocessing algorithm that allows to optimise the solving of the system as indicated above.

Keywords
Feynman integrals, Factorizable systems

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *"D-finite Functions and Beyond: Algorithms, Combinatorics, and Arithmetic"*

D-finiteness, rationality, and height

Jason Bell[1]***, Shaoshi Chen***[2]***, Khoa Nguyen***[3]***, Umberto Zannier***[4] [jpbell@uwaterloo.ca]

[1] Department of Pure Mathematics, University of Waterloo, Waterloo, Canada
[2] KLMM, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing, China
[3] Department of Mathematics and Statistics, University of Calgary, Calgary, Canada
[4] Classe di Scienze Matematiche e Naturali, Scuola Normale Superiore, Pisa, Italy

We discuss the growth of heights of coefficients of a D-finite series, showing that under conditions that ensure sufficiently slow growth, a D-finite series is necessarily rational.

Keywords
Heights, Pólya-Carlson theorem, Growth, Gap theorems

References

[1] J. BELL, K. NGUYEN, U. ZANNIER, D-finiteness, rationality, and height. *Trans. Amer. Math. Soc.* **373**(7), 4889–4906 (2020).
[2] J. BELL, K. NGUYEN, U. ZANNIER, D-finiteness, rationality, and height II: lower bounds over a set of positive density. *arXiv:2205:02145* (2022).

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *"D-finite Functions and Beyond: Algorithms, Combinatorics, and Arithmetic"*

Shift equivalence testing of polynomials and symbolic summation of multivariate rational functions

Shaoshi Chen[1,2]***, Lixin Du***[1,2,3]***, Hanqian Fang***[4] [lx.du@hotmail.com]

[1]KLMM, AMSS, Chinese Academy of Sciences, Beijing, China
[2]School of Mathematical Sciences, University of Chinese Academy of Sciences, Beijing, China
[3]Institute for Algebra, Johannes Kepler University, Linz, Austria
[4]School of Mathematical Sciences, Beihang University, Beijing, China

The Shift Equivalence Testing (SET) of polynomials is deciding whether two polynomials $p(x_1, \ldots, x_n)$ and $q(x_1, \ldots, x_n)$ satisfy the relation $p(x_1+a_1, \ldots, x_n+a_n) = q(x_1, \ldots, x_n)$ for some $a_1, \ldots, a_n$ in the coefficient field. The SET problem is one of basic computational problems in computer algebra and algebraic complexity theory, which was reduced by Dvir, Oliverira and Shpilka in 2014 to the Polynomial Identity Testing (PIT) problem [1]. In this talk, we presents a general scheme for designing algorithms to solve the SET problem which includes Dvir-Oliverira-Shpilka's algorithm as a special case. With the algorithms for the SET problem over integers, we give complete solutions to two challenging problems in symbolic summation of multivariate rational functions, namely the rational summability problem and the existence problem of telescopers for multivariate rational functions. Our approach is based on the structure of isotropy groups of polynomials introduced by Sato in 1960s [2]. Our results can be used to detect the applicability of the Wilf-Zeilberger method to multivariate rational functions.

Keywords
Summability, Telescopers, Isotropy Groups, Shift Equivalences

References

[1] Zeev Dvir, Rafael Mendes de Oliveira, and Amir Shpilka, Testing equivalence of polynomials under shifts. *Electronic Colloquium on Computational Complexity*, 21:3, 2014.

[2] Mikio Sato, Theory of prehomogeneous vector spaces (algebraic part)—the English translation of Sato's lecture from Shintani's note. *Nagoya Mathematical Journal*, 120:1–34, 1990. Notes by Takuro Shintani, Translated from the Japanese by Masakazu Muro.

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *"D-finite Functions and Beyond: Algorithms, Combinatorics, and Arithmetic"*

Galois groups of linear difference-differential equations

Ruyong Feng[1,2], ***Wei Lu***[1,2] [ryfeng@amss.ac.cn]

[1]Key Lab of Mathematics Mechanization, Chinese Academy of Sciences, Beijing, China
[2] University of Chinese Academy of Sciences, Chinese Academy of Sciences,Beijing, China

We consider the following $\sigma\delta$-linear system

$$\begin{cases} \sigma(Y) = AY \\ \delta(Y) = BY \end{cases}, A \in \mathrm{GL}_n(k_0(x)), B \in \mathrm{gl}_n(k_0(x))$$

where A, B satisfy the integrability condition: $\sigma(B)A = \delta(A) + AB$. Here (k_0, δ) is a differential field with algebraically cosed $C = k_0^\delta$, $k_0(x)$ is a $\sigma\delta$-field with shift operator $\sigma(x) = x + 1$. With respect to the above system, there are three algebraic subgroups of $\mathrm{GL}_n(C)$: the $\sigma\delta$-Galois group G of the above system over $k_0(x)$, the σ-Galois group G_{σ,c_1} of $\sigma(Y) = A^{c_1}Y$ over $C(x)$, and the δ-Galois group G_{δ,c_2} of $\delta(Y) = B^{c_2}Y$ over k_0, where $A^{c_1} \in \mathrm{GL}_n(C(x))$ and $B^{c_2} \in \mathrm{gl}_n(k_0)$ are specializations of A and B respectively.

We show that both G_{σ,c_1} and G_{δ,c_2} are algebraic subgroups of G under certain conditions on c_1, c_2, and $G = G_{\sigma,c_1}G_{\delta,c_2}$ for suitable c_1, c_2. These results enable us to reduce the problem of determining $\sigma\delta$-Galois groups to the problems of determining σ-Galois groups and δ-Galois groups. We also give a criterion for testing linear dependence of elements in a simple $\sigma\delta$-ring, which generalizes the classic results for elements in a σ-field or a δ-field and a result for hypexponential elements given by Li et al. 2007.

Keywords
Linear difference-differential equations, Galois groups, Specializations

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *“D-finite Functions and Beyond: Algorithms, Combinatorics, and Arithmetic”*

Symbolic-Numeric Factorization of Differential Operators

Frédéric Chyzak[1]***, Alexandre Goyer***[1]***, Marc Mezzarobba***[2] `[alexandre.goyer@inria.fr]`

[1] Inria, France
[2] CNRS, France

I am going to present a symbolic-numeric Las Vegas algorithm for factoring Fuchsian ordinary differential operators with rational function coefficients. The new algorithm combines ideas of van Hoeij's “local-to-global” method and of the “analytic” approach proposed by van der Hoeven. It essentially reduces to the former in “easy” cases where the local-to-global method succeeds, and to an optimized variant of the latter in the “hardest” cases, while handling intermediate cases more efficiently than both.

Keywords
Linear differential equations, Monodromy, Rigorous Numerics

References

[1] F. CHYZAK; A. GOYER; M. MEZZAROBBA, Symbolic-Numeric Factorization of Differential Operators. In *Proceedings of the 2022 International Symposium on Symbolic and Algebraic Computation*. `https://www.issac-conference.org/2022/`. Not published yet.

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *“D-finite Functions and Beyond: Algorithms, Combinatorics, and Arithmetic”*

Efficient q-integer linear decomposition of multivariate polynomials

Mark Giesbrecht[1], ***Hui Huang***[2], ***George Labahn***[1], ***Eugene Zima***[3] [huanghui@dlut.edu.cn]

[1] Cheriton School of Computer Science, University of Waterloo, Waterloo, Canada
[2] School of Mathematical Sciences, Dalian University of Technology, Dalian, China
[3] Physics and Computer Science, Wilfrid Laurier University, Waterloo, Canada

We present two new algorithms for the computation of the q-integer linear decomposition of a multivariate polynomial. Such a decomposition is essential for the treatment of q-hypergeometric symbolic summation via creative telescoping and also for describing the q-counterpart of Ore-Sato theory. Both of our algorithms require only basic integer and polynomial arithmetic and work for any unique factorization domain containing the ring of integers. Complete complexity analyses are conducted for both our algorithms and two previous algorithms in the case of multivariate integer polynomials, showing that our algorithms have better theoretical performances. A Maple implementation is also included which suggests that our algorithms are much faster in practice than previous algorithms.

Keywords
q-Analogue, Integer-linear polynomials, Polynomial decomposition, Newton polytope, Creative telescoping, Ore-Sato theory

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *"D-finite Functions and Beyond: Algorithms, Combinatorics, and Arithmetic"*

Working with DD-finite functions automatically on SageMath

Antonio Jiménez-Pastor[1] [jimenezpastor@lix.polytechnique.fr]

[1] LIX, CNRS, École Polytechnique, Institute Polytechnique de Paris, Palaiseau, France

In this talk we are going to present the SageMath [5] package `dd_functions` and its latest features concerning DD-finite functions.

DD-finite functions are a natural extension of the holonomic framework. Holonomic (or *D-finite*) functions are formal power series ($f(x) \in \mathbb{K}[[x]]$) that satisfy linear differential equations with polynomials coefficients. These functions form a computable differential ring, namely, the elements can be represented on the computer, and all the ring operations and the derivative can be automatically executed [4]. Hence, they can be use again as coefficients for new differential equations leading to the definition of DD-finite functions.

Definition. [DD-finite] Let $f(x) \in \mathbb{K}[[x]]$. We say that $f(x)$ is *DD-finite* if and only if there is a natural number $d > 0$ and D-finite functions $r_0(x), \ldots, r_d(x)$ ($r_d(x) \neq 0$) such that

$$r_d(x)f^{(d)}(x) + \ldots + r_0(x)f(x) = 0.$$

This definition allows representing DD-finite functions with a finite amount of data since we only need to store the coefficients of the defining differential equation and some initial values $f(0), f'(0), \ldots, f^{(r)}(0)$.

It was shown in [2] that the set of DD-finite functions is also a computable differential ring (as it happened with the D-finite case). In fact, we can extend these results to the case were the coefficients are in a computable differential ring.

Definition. [Differentially definable] Let $R \subset \mathbb{K}[[x]]$ be a differential subring and $f(x) \in \mathbb{K}[[x]]$. We say that $f(x)$ is *differentially definable over* R if there is $d > 0$ and $r_0, \ldots, r_d \in R$ (with $r_d \neq 0$) such that

$$r_d f^{(d)}(x) + \ldots + r_0 f(x) = 0.$$

Theorem [3]. Let $R \subset \mathbb{K}[[x]]$ be a differential subring and let $D(R)$ be the set of all differentially definable functions over R. Then $D(R) \subset \mathbb{K}[[x]]$ is a computable differential ring.

With this result, we can observe that the differentially definable construction can be iterated, obtaining a chain of computable differential rings within $\mathbb{K}[[x]]$:

$$R \subset D(R) \subset D^2(R) \subset \ldots \subset D^n(R) \subset \ldots,$$

and, in this context, is clear that DD-finite functions are $D^2(\mathbb{K}[x])$.

These results were implemented in the SageMath [5] package `dd_functions` that we present in this talk. This software allows to construct any differentially definable ring and manipulate symbolically their elements in an automatic fashion.

This software is publicly available on GitHub[*], and it is constantly updated with the new results concerning DD-finite and differentially functions [1]. It includes:

Structures

- Definition of any differentially definable ring.
- The possibility of working in the chain of $D^n(R)$.
- Create any differentially definable function giving the coefficients for the differential equation and some initial conditions.
- Use an always increasing library of examples coming from special functions.

Operations

- All closure properties are included.
- Composition of differentially definable functions $f(g(x))$ when $g(0) = 0$.
- Computing closure properties keeping the singularities of the differential equations.

Keywords
d-finite; dd-finite; formal power series; SageMath; special functions

References

[1] A. JIMÉNEZ-PASTOR, Simple differentially definable functions. In *ISSAC '21: International Symposium on Symbolic and Algebraic Computation*, Frédéric Chyzak and George Labahn (eds.), 209–216. ACM, 2021.
[2] A. JIMÉNEZ-PASTOR, V. PILLWEIN, A computable extension for D-finite functions: DD-finite functions. *Journal of Symbolic Computations* **94**, 90–104 (2019).
[3] A. JIMÉNEZ-PASTOR, V. PILLWEIN, M. F. SINGER, Some structural results on D^n-finite functions. *Advanced in Applied Mathematics* **117**, 102027 (2020).
[4] M. KAUERS, P. PAULE, *The concrete tetrahedron*. Springer, 2011.
[5] THE SAGE DEVELOPERS, *SageMath, the Sage Mathematics Software System (Version 9.5)*(2021), `https://www.sagemath.org`

[*] `https://www.github.com/Antonio-JP/dd_functions`

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *“D-finite Functions and Beyond: Algorithms, Combinatorics, and Arithmetic”*

Computing Logarithmic Parts by Evaluation Homomorphisms

Hao Du [1], ***Yiman Gao***[2], ***Jing Guo***[2], ***Ziming Li***[2] [zmli@mmrc.iss.ac.cn]

[1] School of Sciences, Beijing University of Posts and Telecommunications, Beijing, China
[2] Key Lab of Math. & Mech., AMSS, Chinese Academy of Sciences, Beijing, China

Let $(K, ')$ be a differential field of characteristic zero, t be transcendental over K and t' belong to $K[t]$. Assume that K and $K(t)$ have the same subfield C of constants. A polynomial p in $K[t]$ is said to be normal if $\gcd(p, p') = 1$. A rational function f in $K(t)$ is said to be simple if it is proper and has a normal denominator.

Let $f \in K(t)$ be simple. Then f has an elementary integral if and only if

$$\int f = c_1 \log g_1 + \cdots + c_m \log g_m$$

for some $c_1, \ldots, c_m$ in the algebraic closure of C and $g_1, \ldots, g_m$ in $K(c_1, \ldots, c_m)(t)$. We call $\{(c_1, g_1), \ldots, (c_m, g_m)\}$ a logarithmic part of f when the above equality holds.

Given a simple function f, known algorithms for determining its logarithmic parts are based on either resultants [1, 6, 7], or subresultants [1, 3, 4], or Gröbner bases [1, 2, 5]. These algorithms need to find a polynomial $r \in K[z]$, where z is a constant indeterminate and r is either the Rothstein-Trager resultant of f [1,6,7] or its squarefree part. Then f has a logarithmic part if and only if the monic associate p of r belongs to $C[z]$. It is time-consuming to compute r when K is a field of multivariate rational functions over C.

We present a new algorithm that computes a candidate $q \in C[z]$ for the monic associate p by evaluation homomorphisms, and attempts to construct a logarithmic part of f using q by algebraic gcd-computation. By a property of residue multiplicities, the algorithm either confirms the non-existence of logarithmic parts or finds a logarithmic part of f. Empirical results illustrate that the algorithm is more efficient than the known algorithms.

Keywords
Elementary integral, Evaluation homomorphism, Logarihtmic part, Simple function

References

[1] M. BRONSTEIN. *Symbolic Integration I: Transcendental Functions*, volume 1 of Algorithms and Computation in Mathematics. Springer-Verlag, Berlin, second edition, 2005.

[2] G. CZICHOWSKI. A note on Gröbner bases and integration of rational functions. *Journal of Symbolic Computation*. 20:163-167, 1995.

[3] D. LAZARD; R. RIOBOO. Integration of rational functions: Rational computation of the logarithmic part. *Journal of Symbolic Computation*. 9:113-116, 1990.

[4] T. MULDERS. A note on subresultants and a correction to the Lazard-Rioboo-Trager formula in rational function integration. *Journal of Symbolic Computation*. 24:45-50, 1997.

[5] CLEMENS G. RAAB. Using Gröbner bases for finding the logarithmic part of the integral of transcendental functions. *Journal of Symbolic Computation*. 47:1290-1296, 2012.

[6] M. ROTHSTEIN. A new algorithm for the integration of exponential and logarithmic functions. In *Proceedings of the 1977 MACSYMA Users Conference*, pages 263-274. NASA Pub. CP-2012, 1977.

[7] B.M. TRAGER. Algebraic factoring and rational function integration. In *Proceedings of SYMSAC'76*, pages 219-226, 1976.

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *“D-finite Functions and Beyond: Algorithms, Combinatorics, and Arithmetic”*

Decision Problems for Second-Order Holonomic Recurrences

Eike Neumann[1]***, Joël Ouaknine***[2]***, James Worrell***[3] [neumaef1@gmail.com]

[1] Department of Computer Science, Swansea University, UK
[2] Max Planck Institute for Software Systems, Saarland Informatics Campus, Germany
[3] Department of Computer Science, Oxford University, UK

We study decision problems for sequences which obey a second-order holonomic recurrence of the form $f(n+2) = P(n)f(n+1) + Q(n)f(n)$ with rational polynomial coefficients, where P is non-constant, Q is non-zero, and the degree of Q is smaller than or equal to that of P. We show that existence of infinitely many zeroes is decidable. We give partial algorithms for deciding the existence of a zero, positivity of all sequence terms, and positivity of all but finitely many sequence terms. If Q does not have a positive integer zero then our algorithms halt on almost all initial values $(f(1), f(2))$ for the recurrence. We identify a class of recurrences for which our algorithms halt for all initial values. We further identify a class of recurrences for which our algorithms can be extended to total ones.

Keywords
Holonomic sequences, Positivity Problem, Skolem Problem

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *"D-finite Functions and Beyond: Algorithms, Combinatorics, and Arithmetic"*

C^2-finite Sequences: A Computational Approach

Philipp Nuspl[1] [philipp.nuspl@jku.at]

[1] Doctoral Program Computational Mathematics, Johannes Kepler University Linz, Austria

We define a class of sequences which satisfy a linear recurrence with coefficients that, in turn, satisfy a linear recurrence with constant coefficients themselves, i.e., are C-finite. These C^2-finite sequences are a natural generalization of P-finite sequences, they form a ring and satisfy additional computational properties [1,2,3]. It turns out that, compared to P-finite sequences, the algorithmic aspects are much more involved and are related to difficult problems in number theory. We give an introduction to these C^2-finite sequences and present an implementation in the computer algebra system SageMath.

Keywords
Difference equations, holonomic sequences, closure properties

References

[1] A. JIMÉNEZ-PASTOR, P. NUSPL, V. PILLWEIN, On C^2-finite sequences. In *ISSAC'21*, F. Chyzak, G. Labahn (eds.), 217–224. 2021.
[2] A. JIMÉNEZ-PASTOR, P. NUSPL, V. PILLWEIN, An extension of holonomic sequences: C^2-finite sequences. In *Journal of Symbolic Computation*. accepted. 2022.
[3] P. NUSPL, V. PILLWEIN, Simple C^2-finite Sequences: a Computable Generalization of C-finite Sequences. In *ISSAC'22*. to appear. 2022.

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *"D-finite Functions and Beyond: Algorithms, Combinatorics, and Arithmetic"*

Factoring differential operators in positive characteristic

Raphaël Pagès [raphael.pages@math.u-bordeaux.fr]

IMB, Université de Bordeaux, Talence, France

We present an algorithm to factor differential operators with coefficients in an algebraic function field K of characteristic p, provided with the usual derivation, as a product of irreducible differential operators with coefficients in K. We make use of tools specific to the characteristic p, such as the p-curvature or the arising central simple algebra structure. In particular we shall see that factoring differential operators ultimately reduces to solving some "p-Ricatti" equations, for which purpose we use tools of algebraic geometry.

Keywords
Differential operators, Factorisation, Positive characteristic, p-curvature, Central simple algebras

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *"D-finite Functions and Beyond: Algorithms, Combinatorics, and Arithmetic"*

Arithmetic of polynomial dynamical systems

Mohammad Sadek [mohammad.sadek@sabanciuniv.edu]

Faculty of Engineering and Natural Sciences, Sabanci University, Istanbul, Turkey

The number theoretic properties of iterations of polynomial maps defined over number fields are governed by the degree of the maps and the degree of the field. Although due attention has been given to iterations of quadratic polynomial maps over number fields of small degree, arithmetic dynamical systems produced by iterations of polynomial maps of higher degrees have not been addressed much in literature. In this talk, we survey some of the old and new results on arithmetic polynomial dynamical systems. The focus will be on algebraic aspects of these systems in the case that the degree of the polynomial map is at least three.

Keywords
Arithmetic dynamics, Dynamical irreducibility, Periodic points

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *"D-finite Functions and Beyond: Algorithms, Combinatorics, and Arithmetic"*

Series defined by quadratic differential equations

Bertrand Teguia Tabuguia [teguia@mis.mpg.de]

Nonlinear Algebra Group, Max Planck Institute for Mathematics in the Sciences, Leipzig, Germany

Differential polynomials of degree at most one annihilate D-finite functions. We consider annihilators of degree at most two and present a general strategy to represent power series solutions of resulting differential equations given enough initial values [1]. Using techniques from algebraic geometry (see [2]), our method extends to representations of Laurent-Puiseux series. Consequently, we can prove identities beyond D-finiteness. However, doing so raises the question of closure properties. Indeed, to show equivalence between two expressions, we may need to establish evidence of the zero-equivalence of their difference; therefore, in a sense, it is relevant to know if the class under consideration contains additive group structures. We present some of our investigations around closure properties with generalization to differential polynomials of degree at most $k \in \mathbb{N}$.

Furthermore, we demonstrate how our method highlights a reverse methodology that finds application in Guessing: recovering a non-D-finite function from a truncation of its power series expansion [3].

Parts of this presentation came from joint work with Wolfram Koepf and Anna-Laura Sattelberger.

Keywords
Differential algebra, Power series representation, Guessing

References

[1] B. Teguia Tabuguia; W. Koepf, On the representation of non-holonomic univariate power series. Submitted, 2021, *arXiv preprint arXiv:2109.09574.*
[2] J. Cano; S. Falkensteiner; J. R. Sendra, Existence and convergence of Puiseux series solutions for autonomous first-order differential equations. *Journal of Symbolic Computation* **108**, 137–151 (2022).
[3] B. Teguia Tabuguia, Guessing with quadratic differential equations. To appear in *ACM communication in Computer Algebra. ISSAC'22 software demonstration* (2022).

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *“D-finite Functions and Beyond: Algorithms, Combinatorics, and Arithmetic”*

q-Difference Equation Systems for Cylindric Partitions

Ali Kemal Uncu[1,2] [akuncu@ricam.oeaw.ac.at]

[1] Austrian Academy of Sciences, Johann Radon Institute for Computational and Applied Mathematics, Linz AT
[2] University of Bath, Department of Computer Science, Bath UK

The cylindric partitions defined by Gessel and Krattenthaler [4] attracted interest after a recent paper by Corteel and Welsh [3]. In this talk, we will look at these objects and their symmetric versions as well as skew double shifted plane partitions. We will especially focus on the coupled q-difference equation systems that these objects are associated with and the difficulties of solving such systems.

Parts of this work is joint with Sylvie Corteel, Jehanne Dousse [2], and Walter Bridges [1].

Keywords
Cylindric Partitions, q-Difference Equations, Computer Algebra

References

[1] W. Bridges; A. K. Uncu, Weighted Cylindric Partitions. https://arxiv.org/abs/2201.03047.
[2] S. Corteel; J. Dousse; A. K. Uncu, Cylindric Partitions and some new A_2 Rogers–Ramanujan Identities. *Proc. Amer. Math. Soc.* **150**, 481-497 (2022).
[3] S. Corteel; T. Welsh, The A_2 Rogers–Ramanujan identities revisited, *Annals of Comb.* **23**, 683-–694 (2019).
[4] I.M. Gessel; C. Krattenthaler, Cylindric partitions, *Trans. Amer. Math. Soc.* **349**, 429–479 (1997).

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *“Algebraic and Geometric Methods in Coding Theory”*

Computational classification of symplectic 4-dimensional semifields over finite fields

Michel Lavrauw[1]***, John Sheekey***[2] [michel.lavrauw@sabanciuniv.edu]

[1] Faculty of Engineering and Natural Sciences, Sabancı University, Tuzla, Istanbul 34956, Turkey
[2] School of Mathematics and Statistics, University College Dublin, Belfield, Dublin 4, Ireland

We will report on the classification of symplectic 4-dimensional semifields over $\mathbb{F}_q$, for $q \leq 9$ from [1]. This classification extends (and confirms) the previously obtained classifications for $q \leq 7$. The classification is obtained by classifying all symplectic semifield subspaces in $\mathrm{PG}(9, q)$ for $q \leq 9$ up to K-equivalence, where $K \leq \mathrm{PGL}(10, q)$ is the lift of $\mathrm{PGL}(4, q)$ under the Veronese embedding of $\mathrm{PG}(3, q)$ in $\mathrm{PG}(9, q)$ of degree two. Our results imply the non-existence of non-associative symplectic 4-dimensional semifields for q even, $q \leq 8$. For q odd, and $q \leq 9$, our results imply that the isotopism class of a symplectic non-associative 4-dimensional semifield over $\mathbb{F}_q$ is contained in the Knuth orbit of a Dickson commutative semifield.

Keywords
Semifield, Veronese embedding, Isotopism class

References

[1] M. LAVRAUW, J. SHEEKEY, *Symplectic 4-dimensional semifields of order* 8^4 *and* 9^4. Preprint.

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *“Algebraic and Geometric Methods in Coding Theory”*

Divisible codes and few-weight codes in the rank metric

John Sheekey[1]***, Olga Polverino***[2]***, Paolo Santonastaso***[2]***, Ferdinando Zullo***[2] [john.sheekey@ucd.ie]

[1] School of Mathematics and Statistics, University College Dublin, Ireland
[2] Università degli Studi della Campania “Luigi Vanvitelli”, Caserta, Italy

Linear codes in which the weights of the codewords are restricted in some way have been frequently studied in the Hamming metric; for example e-divisible codes, where all weights are divisible by an integer $e > 1$, and two-weight codes, where the set of weights of nonzero codewords has cardinality two.

Codes in the rank metric have been studied with increasing intensity in recent years. In this work we aim to construct and characterise divisible codes with certain properties, as well as study one-, two-, and three-weight codes.

Keywords
Rank-metric codes, divisible, two-weight

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *“Algebraic and Geometric Methods in Coding Theory”*

Construction of Subspace Codes using Evaluation

Joachim Rosenthal[1] [rosenthal@math.uzh.ch]

[1] Institute of Mathematics, University of Zurich, Winterthurerstrasse 190, 8057 Zurich.

A constant dimension subspace code can be viewed geometrically as a subset of the Grassmann variety defined over a finite field.

There exist few algebraic constructions for constant dimension subspace codes. A major technique is the 'lifting technique' of a rank metric code with a good distance. For rank metric codes exist several good algebraic constructions. First and for most one should mention the technique of constructing Gabidulin codes which can be seen as the image of a linear space of linearized functions under an evaluation map. The technique of constructing Gabidulin codes naturally generalizes the construction of AG-codes such as Reed-Solomon codes and more general geometric Goppa codes.

In this talk we present a new idea on how one can construct excellent subspace codes by evaluating points on a rational curve in the Grassmannian.

Keywords
Subspace codes, rank metric codes, evaluation codes.

References

[1] HORLEMANN-TRAUTMANN, A. AND ROSENTHAL, J., *Constructions of constant dimension codes.* In M. Greferath, M. Pavcevic, N. Silberstein, and M. Vazquez-Castro (eds.), *Network Coding and Subspace Design*, Signals and Communication Technology, 25–42. Springer Verlag, 2018.

[2] MANGANIELLO, F., GORLA, E., AND ROSENTHAL, J., *Spread codes and spread decoding in network coding.* In *Proceedings of the 2008 IEEE International Symposium on Information Theory*, 851–855. Toronto, Canada, 2008.

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *"Algebraic and Geometric Methods in Coding Theory"*

Protograph-based LDPC codes with chordless short cycles and large minimum distance

Farzane Amirzade[1], ***Daniel Panario***[1], ***Mohammad-Reza Sadeghi***[2]

[1] School of Mathematics and Statistics, Carleton University, Ottawa, Canada
[farzaneamirzadedana@cunet.carleton.ca, daniel@math.carleton.ca]
[2] Faculty of Mathematics and Computer Science, Amirkabir University of Technology, Tehran, Iran [msadeghi@aut.ac.ir]

Quasi-cyclic low-density parity-check codes (QC-LDPC codes) are an essential category of LDPC codes that have simple implementation and favorable performance. One of the most important representations for codes is the Tanner graph in which the length of the shortest cycles, girth, has been known to influence the code performance. Since Tanner graphs with short cycles do not produce good results, constructions which lead to the existence of 4-cycles in their Tanner graphs are avoided. Indeed, in almost all of the algebraic-based constructions proposed up to now Tanner graph has girth at least 6.

Another phenomenon that influences the performance of LDPC codes are trapping sets. An (a, b) trapping set is a subgraph of the Tanner graph which is induced by a variable nodes in the set and their check node neighbors, with b check nodes of odd degrees (the unsatisfied check nodes) and an arbitrary number of even degree check nodes (the satisfied check nodes). Empirical results show that among all trapping sets, the most harmful ones are those with check nodes of degree 1 or 2. These are called elementary trapping sets (ETSs).

Controlling small size trapping sets and short cycles can result in LDPC codes with large minimum distance $d_{\min}$. We prove that short cycles with a chord are the root of several trapping sets, and eliminating these cycles increases $d_{\min}$. We show that the lower bounds on $d_{\min}$ of an LDPC code with chordless short cycles, girth 6, and column weights γ is 2γ. This is a significant improvement compared to the existing bound $\gamma + 1$.

Several exponent matrices of protograph-based LDPC codes with chordless short cycles are proposed for any type of protographs, single-edge and multi-edge. These numerical results as well as simulations show that the removal of short cycles with a chord improves previous results in the literature.

Keywords
LDPC codes, girth, Tanner graph, elementary trapping set, chordless cycles, minimum distance.

Ordered Covering Arrays and NRT-metric Covering Codes

Lucia Moura lmoura@uottawa.ca

University of Ottawa, Ottawa, Canada

Ordered covering arrays generalize both ordered orthogonal arrays and covering arrays, which are well-studied combinatorial designs. Classical codes using the Hamming metric can be generalized to codes with a poset metric. The Niederreiter-Rosenbloom-Tsfasman (NRT) metric corresponds to posets that are the disjoint union of chains of the same size. In this talk, we discuss ordered covering arrays and their use in upper bounds for NRT-metric covering codes. This talk is based on joint work with André Guerino Castoldi, Emerson Luiz do Monte Carmelo, Daniel Panario and Brett Stevens [1,2].

Keywords
combinatorial designs, covering codes, covering arrays

References

[1] A. Castoldi; E. Monte Carmelo; L. Moura; D. Panario; B. Stevens, *Bounds on covering codes in RT spaces using ordered covering arrays*. In: *Algebraic Informatics. CAI 2019.*, Ciric, M., Droste, M., Pin, JE. (eds.), Lecture Notes in Computer Science, vol 11545. Springer, Cham. 2019.
[2] A. Castoldi; E. Monte Carmelo; L. Moura; D. Panario; B. Stevens, *Ordered covering arrays and upper bounds on covering codes in NRT spaces*. preprint 2022.

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *“Algebraic and Geometric Methods in Coding Theory”*

Better CRC Codes

Anton Betten

Department of Mathematics, Kuwait University, Kuwait

CRC Codes are used to detect communication errors, for instance in TCP/IP Internet traffic. The standard is CRC32, which adds a 32 bit checksum to the information packet. It has been observed by Partridge et.al. that certain errors may slip by this check sum, leading to corrupt data transfer. We will present some ideas for better checksums. Our approach is based on BCH-codes over extension fields in characteristic two. The check sum will be longer, leading to a slightly lower information rate, but the error detection is significantly stronger, in particular for the type of errors that appear frequently.

This is joint work with Craig Partridge and Joseph Riva.

Keywords
CRC code, check sum, CRC polynomial, Finite Field

References

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *"Algebraic and Geometric Methods in Coding Theory"*

Constructions of new matroids and designs over $\mathbb{F}_q$

Eimear Byrne[1]***, Michela Ceria***[2]***, Sorina Ionica***[3]***, Relinde Jurrius***[4]***, Elif Saçikara***[5] [rpmj.jurrius@mindef.nl]

[1] University College Dublin, Ireland
[2] Politecnico di Bari, Italy
[3] Netherlands Defence Academy, The Netherlands
[4] University of Picardie Jules Verne, France
[5] University of Zürich, Switzerland

A *perfect matroid design (PMD)* is a matroid whose flats of the same rank all have the same size. As the name suggest, these matroids give rise to certain designs, and in the literature this construction is used to find new designs. The aim of this work is to establish a q-analogue of this construction.

We will introduce the q-analogue of a PMD and its properties. In order to do that, we first define a q-matroid in terms of its flats. We show that q-Steiner systems are examples of q-PMD's, just like Steiner systems are examples of PMD's. We use the q-matroid structure to construct subspace designs from q-Steiner systems. We apply this construction to known q-Steiner systems and discuss the designs coming from it.

Keywords
q-analogue, q-matroid, subspace design

References

[1] E. Byrne; M. Ceria; S. Ionica; R. Jurrius; E. Saçikara, Constructions of new matroids and designs over $\mathbb{F}_q$. https://arxiv.org/abs/2005.03369 (2020).

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *"Algebraic and Geometric Methods in Coding Theory"*

Critical Problem, q-Polymatroids and Rank-Metric Codes

Gianira N. Alfarano[1], ***Eimear Byrne***[2] [gianiranicoletta.alfarano@math.uzh.ch]

[1] Institute of Mathematics, University of Zurich, Zurich,
Switzerland
[2] School of Mathematics and Statistics, University College Dublin,
Belfield, Ireland

In classical combinatorics, polymatroids have been introduced as an extension of the concept of matroid. There are many known connections between linear codes and matroids and many invariant in coding theory are also matroid invariants. q-Matroids and q-polymatroids are the q-analogue of matroids and polymatroids. These objects have gained a lot of interest among an increasing number of researchers, especially in the last few years, due to their connection with rank-metric codes. In particular, in [3] it has been shown that to an $\mathbb{F}_q$-linear rank metric code $\mathcal{C} \leq \mathbb{F}_q^{n\times m}$ it can be associated a q-polymatroid $M_{\mathcal{C}}$ and when $\mathcal{C}$ is also $\mathbb{F}_{q^m}$-linear, $M_{\mathcal{C}}$ is a q-matroid; see [2].

In this talk we will show some recent results on the invariants of q-polymatroids and rank-metric codes. One of these results lead to the solution of the q-analogue of the classical Critical Problem, proposed by Crapo and Rota in [1]. We will make use of the characteristic polynomial of a q-polymatroid as a basic tool for this result. Finally, we will provide the coding theoretic interpretation and we will partially solve it for *maximum rank distance* codes.

Keywords
Critical problems, q-polymatroids, rank-metric codes.

References

[1] H. CRAPO, G.-C. ROTA, *On the foundations of combinatorial theory: Combinatorial geometries*. MIT Press, 1970.

[2] R. JURRIUS, R. PELLIKAAN, Defining the q-Analogue of a Matroid. *The Electronic Journal of Combinatorics*, (2018)

[3] E. GORLA, R. JURRIUS, H. LÓPEZ, A. RAVAGNANI., Rank-metric codes and q-polymatroids. *Journal of Algebraic Combinatorics*, **52**(1), 1–19 (2020).

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *"Algebraic and Geometric Methods in Coding Theory"*

On the geometry of $(q+1)$-arcs of PG$(3,q)$, q even

Michela Ceria[1]***, Francesco Pavese***[1] [michela.ceria@poliba.it]

[1] Department of Mechanics, Mathematics and Management, Politecnico di Bari, Italy

Let us consider the projective space $\mathrm{PG}(3,q)$ of dimension three over the finite field $\mathbb{F}_q$, for q a power of a prime. We call $(q+1)$-arc of $\mathrm{PG}(3,q)$ a set of $q+1$ points of $\mathrm{PG}(3,q)$ such that no four of them are coplanar. In this talk we focus on the case $q=2^n$, in which a $(q+1)$-arc is projectively equivalent to

$$\mathcal{A} = \{P_t = (1, t, t^{2^h}, t^{2^h+1}) \mid t \in \mathbb{F}_q\} \cup \{(0,0,0,1)\},$$

where $\gcd(n,h)=1$ and it is also projectively equivalent to

$$\bar{\mathcal{A}} = \{(1, t, t^{2^{n-h}}, t^{2^{n-h}+1}) \mid t \in \mathbb{F}_q\} \cup \{(0,0,0,1)\}.$$

For $q \geq 5$, the group leaving $\mathcal{A}$ invariant, that we denote by G_h, is a subgroup of $\mathrm{PGL}(4,q)$ isomorphic to to $\mathrm{PGL}(2,q)$.

In the case $h=1$, the $(q+1)$-arc $\mathcal{A}$ is called *twisted cubic*; it has been deeply studied in literature, and, in particular, so is the action of its group G_1 on points, lines and planes. Besides being important from a geometrical point of view, its relevance relates also to its connection to coding theory and for example to asymptotically optimal multiple covering codes [1].

In this talk, we deal with the orbits of the group G_h on points, lines and planes of $\mathrm{PG}(3,q)$. In particular, we show that, similarly to what happens for the twisted cubic, there are five orbits on points and planes. Moreover, the orbits on lines are $2q+7+\xi$, where $q \equiv \xi \mod 3$. This proves, in even characteristics, Conjecture 8.2 of [2].

We conclude examining the point-line incidence matrix for the case of the twisted cubic.

Keywords
$(q+1)$-arc, twisted cubic, incidence matrix

References

[1] D. Bartoli; A.A. Davydov; S. Marcugini; F. Pambianco, *On planes through points off the twisted cubic in PG(3, q) and multiple covering codes.* Finite Fields Appl., 67

(2020), 101710.
[2] A.A. DAVYDOV; S. MARCUGINI; F. PAMBIANCO, *Twisted cubic and orbits of lines in* $\mathrm{PG}(3, q)$ II, *arXiv 2112.14803v1*, preprint, 2021.

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *“Algebraic and Geometric Methods in Coding Theory”*

Trifferent codes and affine blocking sets

Anurag Bishnoi[1]***, Dion Gijsiwijt***[1]***, Jozefien D’haesleer***[2]***, Aditya Potukuchi***[3] [A.Bishnoi@tudelft.nl]

[1] Department of Applied Mathematics, Delft University of Technology, Delft, Netherlands
[2] Department of Mathematics: Analysis, Logic and Discrete Mathematics, Ghent University, Ghent, Belgium
[3] Department of Mathematics, Statistics, and Computer Science, University of Illinois Urbana-Champaign, Chicago, USA

Trifferent codes, also known as perfect 3-hash codes, are subsets of C of $\{0,1,2\}^n$ such that for any three distinct codewords in C, there is a common coordinate position where all of these codewords have different values. When $\{0,1,2\}$ is identified with $\mathbb{F}_3$ and C is a linear subspace of $\mathbb{F}_3^n$, then it is called a linear trifferent code. Studying the maximum possible size of trifferent codes of length n, as a function of n, is one of the classic open problems in both coding theory and extremal combinatorics [1,2]. The trivial upper bound of $c\left(\frac{3}{2}\right)^n$ has not been improved despite considerable effort, except for the constant c. The best known lower bound is also exponential but with a smaller base of the exponent. Recently, Pohoata and Zakharaov [3] studied linear trifferent codes and showed a much stronger upper bound on their size. In this talk we will see further improvements to their bound and prove exponential lower bounds. We obtain these results by exploiting a connection of this problem with certain affine blocking sets. In addition to this connection, we use the MRRW bound from coding theory to obtain our new upper bounds on linear trifferent codes. For the lower bound we use a probabilistic construction. We also propose a natural problem in finite geometry, where explicit constructions can potentially lead to the best known explicit lower bounds on trifferent codes.

Keywords
Trifferent codes, Perfect k-hash codes, Blocking sets

References

[1] V. GURUSWAMI; A. RIAZANOV, Beating Fredman-Komlós for perfect k-hashing. In *46th International Colloquium on Automata, Languages, and Programming (ICALP 2019)*, , Schloss DagstuhlLeibniz-Zentrum fuer Informatik, 2019.
[2] J. KÖRNER, *Coding of an information source having ambiguous alphabet and the entropy of graphs.* 6th Prague Conference on Information Theory, 411–425, 1973.
[3] C. POHOATA; D. ZAKHAROV, On the trifference problem for linear codes. *arXiv* (2105.00122), (2021).

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *“Algebraic and Geometric Methods in Coding Theory”*

Cameron–Liebler type sets and completely regular codes

Morgan Rodgers[1] [morgan.rodgers@istinye.edu.tr]

[1] Mathematics Department, Istinye University, Istanbul, Turkey

The notion of a *completely regular code* was initially given by Delsarte [1] as a generalization of a perfect code. Delsarte defined these not only for codes in the Hamming graphs, but more generally for vertex subsets of any arbitrary distance regular graph.

One important family of completely regular codes in the Grassmann graphs is given by the *Cameron–Liebler sets of k-spaces*. A Cameron–Liebler line class in $\mathrm{PG}(3,q)$ can be defined as a set $\mathcal{L}$ of lines whose characteristic vector lies in $\mathrm{row}(A)$, where A is the point-line incidence matrix of $\mathrm{PG}(3,q)$ [2]. These objects provide examples of completely regular codes in the Grassmann graph $\mathcal{G}_q(4,2)$. They are also connected to collineation groups of $\mathrm{PG}(3,q)$ having the same number of orbits on points and lines, as well as to symmetric tactical decompositions of the point-line design $\mathrm{PG}(3,q)$.

The concept of a Cameron–Liebler line class has also been generated to sets of k-spaces in $\mathrm{PG}(n,q)$ for arbitrary n and k, and we again get imporant examples of completely regular codes in the Grassmann graph $\mathcal{G}_q(n+1,k+1)$ from these objects.

In this talk, we will look at the known results on Cameron–Liebler sets in these contexts, and explore in detail the connection to completely regular codes. We will also look at Cameron–Liebler sets in the context of generators in a finite classical polar space, as vertex sets in the dual polar graphs.

Keywords
Finite Geometry, Cameron–Liebler sets, Completely regular codes

References

[1] P. DELSARTE, An algebraic approach to the association schemes of coding theory. *Phillips Res. Rep. Suppl.* **10**, 1–97 (1973).
[2] P.J. CAMERON, R.A. LIEBLER, Tactical decompositions and orbits of projective groups. *Linear Algebra Appl.* **46**, 91–102 (1982).

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *“Algebraic and Geometric Methods in Coding Theory”*

Mutually Orthogonal Latin Squares based on e-Klenian polynomials

Jaime Gutierrez[1]***, Jorge Jimenez Urroz***[2] [jaime.gutierrez@unican.es]

[1] Dept. Matemática Aplicada y Computación, Universidad de Cantabria, Santander, Spain
[2] Departamento de Matematicas, Universitat Politécnica Catalunya, Barcelona, Spain

A latin square of order $t \in \mathbb{N}$ is an $t \times t$ matrix L with entries from a set T of size n such that each element of T occurs exact once in every row and every column of L, see [3].

Two Latin squares L_1 and L_2 of order t are orthogonal if by superimposing them one obtains all ordered pairs $(t_i, t_j) \in T^2$, $(i, j = 1, \dots, t)$, and mutually orthogonal latin squares (MOLS) are sets of Latin squares that are pairwise orthogonal. The construction of MOLS is a notoriously difficult combinatorial problem and it is one of the most studied research topics in design theory [5]. This interest is also due to the numerous applications that MOLS have in other fields such as cryptography [6], coding theory and many others [2].

In this talk we investigate new constructions of MOLS of prime p and prime power $q = p^r$ size, based on local permutation polynomials. It is known every Latin square can be represented by a local permutation polynomial, $f(x, y) \in \mathbb{F}_q[x, y]$ with coefficients in a finite field $\mathbb{F}_q$ with q elements, that is, defines two permutations $f(a, y)$ and $f(x, a)$ in in $\mathbb{F}_q$ for any $a \in \mathbb{F}_q$. Permutation polynomials is a very well known area with a lot of interest in mathematics and computer science community, see the excellent bible [4]. After introducing the local permutation polynomials based on symmetric subgroups without fixed points, called e-Klenian polynomials [1], we provide a big family of MOLS.

Keywords
Mutually orthogonal latin squares, local permutation polynomials, finite fields.

References

[1] J. GUTIERREZ, J. J. URROZ, *Local permutation polynomials and the action of e-Klenian groups*, arXiv:2205.0015, 2022.
[2] A.D. KEEDWELL, J. DÉNES. *Latin Squares and their Applications.* Elsevier, Amsterdam 2015.
[3] C. F. LAYWINE, G. L. MULLEN. *Discrete Mathematics Using Latin Squares*, John Wiley & Sons, 1998.
[4] R. LIDL, H. NIEDERREITER, *Finite Fields*, 2nd edn., Encyclopedia Math. Appl., vol.20,

Cambridge University Press, Cambridge, 1997.
[5] MONTGOMERY D.C. *Design and Analysis of Experiments*. Wiley, Hoboken 2017.
[6] D. R. STINSON. *Combinatorial characterizations of authentication codes*. Des. Codes Cryptogr. (1992) 2(2), 175–187.

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *“Algebraic and Geometric Methods in Coding Theory”*

On Optimal Binary Linear Complementary Pair of Codes

Cem Güneri [cem.guneri@sabanciuniv.edu]

Faculty of Engineering and Natural Sciences, Sabancı University, 34956, İstanbul, Turkey

A pair of linear codes (C, D) of length n over $\mathbb{F}_q$ is called a linear complementary pair (LCP) if their direct sum $C \oplus D$ yields $\mathbb{F}_q^n$. We call (C, D) an $[n, k]$ LCP of codes if $\dim C = k$. LCP of codes have drawn attention in recent years due to cryptographic applications via direct sum masking scheme, which is proposed as a countermaeaure against side channel and fault injection attacks ([1,2,5]).

The security parameter of an LCP of codes (C, D) is defined as $\min\{d(C), d(D^{\perp})\}$. If we denote by $d_L(n, k)$ the largest minimum distance of an $[n, k]$ linear code over $\mathbb{F}_q$, and by $d_{LCP}(n, k)$ the highest security parameter for an $[n, k]$ LCP of codes over $\mathbb{F}_q$, it is clear that $d_{LCP}(n, k) \leq d_L(n, k)$ for all q. Carlet et al. showed in [3] that $d_L(n, k) = d_{LCP}(n, k)$ for all n and k, if $q \geq 3$ (i.e. there exists optimal LCP of codes over $\mathbb{F}_q$, if $q \geq 3$). For binary linear codes, they showed in the same article that $d_{LCP}(n, k) \geq d_L(n, k) - 1$. So, the best security parameter problem is open for further study in the case of binary LCP of codes.

It has been proved in [4] that the binary LCP of codes are optimal in the following broad cases:

- For any dimension $k \geq 2$ and length n congruent to 0 or 1 modulo $(2^k - 1)$,
- For any length n and dimension $2 \leq k \leq 4$, with the exception of two parameters: $(n, k) = (4, 3)$ and $(8, 4)$.

The talk will review the problem, present the results of [4] and the ideas involved in obtaining them, as well as some more recent observations, which yield further optimal binary LCP's using a family of Griesmer codes.

Part of the results have been obtained in collaboration with W.-H. Choi, J.-L. Kim and F. Özbudak. Supported by a bilateral cooperation program between Korea and Turkey, under TÜBİTAK grant with the project code 120N932.

Keywords
Linear complementary pairs, optimal codes, Griesmer codes.

References

[1] J. Bringer; C. Carlet; H. Chabanne; S. Guilley; H. Maghrebi, Orthogonal direct sum masking: A smartcard friendly computation paradigm in a code, with builtin protection against side-channel and fault attacks. In *WISTP, Heraklion, Crete, LNCS vol. 8501*, 40–56, 2014.

[2] C. Carlet; S. Guilley, Complementary dual codes for counter-measures to side-channel attacks. *Adv. Math. Commun.* **10**, 131–150 (2016).

[3] C. Carlet; S. Mesnager; C. Tang; Y. Qi, On σ-LCD codes. *IEEE Trans. Inf. Theory.* **65**, 1694–1704 (2019).

[4] W.-H. Choi; C. Güneri̇; J.-L. Kim; F. Özbudak, Optimal binary linear complementary pairs of codes. *submitted.*

[5] X.T. Ngo; S. Bhasin; J.-L. Danger; S. Guilley; Z. Najm, Linear complementary dual code improvement to strengthen encoded circuit against hardware Trojan horses. In *IEEE International Symposium on Hardware Oriented Security and Trust (HOST), Washington, DC, USA*, 82–87, 2015.

On LCP of 1-generator QC codes

Zohreh Aliabadi[1] [zaliabadi@sabanciuniv.edu]

[1] Faculty of Engineering and Natural Sciences, Sabanci university, Istanbul, Turkey

Linear complementary dual (LCD) codes were introduced by Massey in 1992. A linear code C is LCD if it intersects its dual trivially. A characterization of LCD QC codes has been given by Güneri, et.al. in 2016 through the constituents of QC codes.
Linear complementary pair (LCP) of codes, can be considered as a generalization of LCD codes. A pair (C, D) of linear codes is called LCP of codes if $C \oplus D = \mathbb{F}_q^n$, C and D intersect trivially. Such codes have been studied by Carlet, et. al. It has been shown that if (C, D) is LCP of QC codes, then it does not necessary implies that C and $D^\perp$ are equivalent. We studied the 1-generator QC codes. A characterization of such codes is given in terms of their generator and parity check polynomials. Moreover, LCP of this family is characterized via the generator elements of C and D. If (C, D) is LCP of cyclic codes, or more generally abelian codes, it has been shown that C and $D^\perp$ are equivalent codes. However this is not true for general linear codes or quasi cyclic codes. Moreover, equivalence of C and $D^\perp$ is studied for an LCP of 1-generator quasi cyclic codes. This is a joint work with Cem Güneri[1], Tekgül Kalaycı[1].

Keywords
Linear Complementary Dual, Linear Complementary pair, Quasi Cyclic Code, 1-generator Quasi Cyclic codes, Code Equivalence

References

[1] C. CARLET, C. GÜNERI, F. ÖZBUDAK, B. ÖZKAYA, P. SOLE, *On linear complementary pairs of codes,*.IEEE Transactions on Information Theory, vol. 64, 6583-6589,(2018).
[2] C. GÜNERI, B. ÖZKAYA, P. SOLE, *Quasi-cyclic complementary dual codes.* Finite Fields and Their Applications, vol. 42, 67-80, (2016).
[3] S. LING AND P. SOLE,, *On the algebraic structure of quasi-cyclic codes I: Finite Fields.* IEEE-IT, Vol.47, No. 7, November (2001) 2751-2760.
[4] S. LING AND P. SOLE,, *On the algebraic structure of quasi-cyclic codes III: generator theory.* ,IEEE Trans. Inf. Theory 51 (2005) 2692-2700.
[5] J.L. MASSEY, *Linear codes with complementary duals.* Discrete Math. 106-107 (1992).

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *‘Parametric Polynomial Systems”*

A deterministic method for computing Bertini type invariants of parametric ideals

Shinichi Tajima[1]***, Katsusuke Nabeshima***[2] [tajima@math.tsukuba.ac.jp]

[1] Graduate School of Science and Technology, Niigata Univ., Ikarashi, Niigata, Japan
[2] Department of Applied Mathematics,Tokyo Univ. of Science, Kagurazaka, Tokyo, Japan

Let us start by recalling the classical theorem of Bertini. Let X be a smooth algebraic variety in a projective space $\mathbb{P}^n$. Let $H \subset \mathbb{P}^n$ be a hyperplane. Then, the theorem of Bertini says that the hyperplane section $X \cap H$ is smooth, if H is *general*. General objects are ubiquitous in many fields. In fact, especially in algebraic geometry, there are many properties, concepts and invariants that involve generality conditions. In this paper, w call such a kind of invariant Bertini type invariant. It is difficult to compute Bertini type invariants for singular varieties because of genericities. There are two major methods for computing Bertini invariants. One is the use of random numbers. The other method utilized tools from numerical algebraic geometry, the software Bertini developed by Daniel J. Bates et al [2]. Both methods are widely used, however, they are not deterministic.

We propose an alternative, deterministic method for computing Bertini type invariants. The key of our approach is the Gröbner basis computation with coefficients in the field of rational functions of new auxiliary indeterminates. For the case that a family of varieties or ideals depending on deformation parameters are given. Computing parameter dependency of Bertini type invariants is of fundamental importance. In this talk, we address such parametric cases and show that by utilizing the theory of comprehensive Gröbner systems, our approach can be extended to treat parametric cases.

Here we give an example to illustrate a role of auxiliary indeterminates in our approach.

Chern-Schwartz-MacPherson class

Let $\phi : \mathbb{P}^n \longrightarrow \mathbb{P}^n$ be a rational map. Let $g_i = \mathrm{card}(\phi^{-1}(\mathbb{P}^{n-i}) \cap \mathbb{P}^i)$, where $\mathbb{P}^{n-i}$ and $\mathbb{P}^i$ are *general* planes of dimension $n-i$ and i respectively. Then, $g = (g_0, g_1, g_2, \ldots, g_n)$ is called the projective degrees of the map ϕ. (See [6].)

Let $V = V(f)$ be a hypersurface of $\mathbb{P}^n$, where f is a defining polynomial of V. Let $c_{SM}(V)$ be the Chern-Schwartz-MacPherson class of V. (See [7].)

Theorem (P. Aluffi[1]) Let $g = (g_0, g_1, \ldots, g_n)$ be the projective degrees of the polar map

$\phi : \mathbb{P}^n \longrightarrow \mathbb{P}^n$ defined to be

$$\phi : p \mapsto (\frac{\partial f}{\partial z_0}(p), \frac{\partial f}{\partial z_1}(p), \cdots, \frac{\partial f}{\partial z_n}(p))$$

Then,

$$c_{SM}(V) = (1+h)^{n+1} - \sum_{j=0}^{n} g_j(-h)^j(1+h)^{n-j} \in \mathrm{A}_*(\mathbb{P}^n)$$

holds, where h is the class of a hyperplane defined by a general linear form and $\mathrm{A}_*(\mathbb{P}^n)$ is the Chow ring of the projective space $\mathbb{P}^n$.

The next result is due to M. Helmer [4].

Proposition (M. Helmer) Let $S = 1 - s\sum_{j=0}^{n} c_j \frac{\partial f}{\partial z_j},\ L_A = 1 - \sum_{j=0}^{n} r_j z_j$ and

$P_k = \sum_{j=0}^{n} a_{j,k} \frac{\partial f}{\partial z_j},\ L_k = \sum_{j=0}^{n} b_{j,k} z_j,\ k = 1, 2, \ldots, n.$

Assume that all the coefficients $a_{j,k}, b_{j,k}, c_j, r_j$ are *general*. Then the projective degrees $g = (g_0, g_1, g_2, \ldots, g_n)$ of the polar map defined in the above theorem are given by

$g_i = \dim_K(K[z_0, z_1, \ldots, z_n, s]/(P_1 + P_2 + \cdots + P_i + L_1 + L_2 + \cdots + L_{n-i} + L_A + S)).$

M. Helmer utilized probabilistic method and tools from numerical algebraic geometry for computing projective degrees and he obtained an algorithm for computing Chern-Schwartz-MacPherson classes [4].

Now, we regard $a_{j,k}, b_{j,k}, c_j, r_j$ as indeterminates and set $u = (a_{j,k}, b_{j,k}, c_j, r_j), j, k = 1, 2, \ldots, n$ and $x = (z_1, z_2, \cdots, z_n, s)$. Let $K(u)[x]$ denote the polynomial ring with coefficients in $K(u)$, where $K(u)$ is the fields of rational functions of u. We have the following result.

Proposition Let G_i be a Gröbner basis, in the ring $K(u)[x]$, of the ideal generated by $P_1, P_2, \ldots, P_i, L_1, L_2, \ldots, L_{n-i}, L_A$. Then, $g_i = \dim_{K(u)}(K(u)[x]/(G_i)), i = 1, 2, \ldots, n$ hold.

The above proposition togather with the theorem of Aluffi allow us to construct a deterministic method for computing Chern-Schwartz-MacPherson classes!!

Comprehensive Gröbner systems with auxiliary indeterminates

Let $x = \{x_1, x_2, \ldots, x_n\}, t = \{t_1, t_2, \ldots, t_m\}, u = \{u_1, u_2, \ldots, u_\ell\}$ and let $(K(u)[t][x]$ denote the ring of polynomials with coefficients in $K(u)[t]$. Here we regard x as main variables, t as parameters and u as auxiliary indeterminates.

Let $\overline{K(u)}$ be an algebraic closure of the field $K(u)$ of rational functions. For an arbitrary $\bar{t} \in \left(\overline{K(u)}\right)^m$, the specialization homomorphism

$$\sigma_{\bar{t}} : (K(u)[t])[x] \longrightarrow \overline{K(u)}[x]$$

is defined as the map that substitutes $\bar{t}$ into m variables t. For $G \subset (K(u)[t])\{x\}$, $\sigma_{\bar{t}}(G) = \{\sigma_{\bar{t}}(g)|g \in G\} \subset \overline{K(u)}\{x\}$. For $g_1, \dots, g_r \in K(u)[t]$,

$$V_{\overline{K(u)}}(g_1, \dots, g_r) = \left\{\bar{t} \in \left(\overline{K(u)}\right)^m \mid g_1(\bar{t}) = \cdots = g_r(\bar{t}) = 0\right\}.$$

We call an algebraic constructible set of the form $V_{\overline{K(u)}}(g_1, \dots, g_r)\backslash V_{\overline{K(u)}}(g'_1, \dots, g'_{r'})$, a stratum. Notations $A_1, A_2, \dots, A_r$ are frequently used to represent strata.

Definition Fix a term ordering $\succ_x$ on $K[x]$. Let $F \subset (K(u)[t])[x]$, $A_1, \dots, A_r \subset \left(\overline{K(u)}\right)^m$, $S_1, \dots, S_r \subset (K(u)[t])[x]$. If a finite set $\mathcal{G} = \{(A_1, S_1), \dots, (A_r, S_r)\}$ of pairs satisfies the properties such that (i) for $i \neq j$, $A_i \cap A_j = \emptyset$, and (ii) for all $\bar{t} \in A_i$ and $g \in S_i$, $ht_{\succ_x}(g) = ht_{\succ_x}(\sigma_{\bar{t}}(g))$ and $\sigma_{\bar{t}}(S_i)$ is a Gröbner basis of $\langle\sigma_{\bar{t}}(F)\rangle$ in $\overline{K(u)}[x]$, ($ht_{\succ_x}$ stands for the head term) then, $\mathcal{G}$ is called a comprehensive Gröbner system (CGS) of $\langle F\rangle$ over $\overline{K(u)}$ on $A_1 \cup \cdots \cup A_r$. We call a pair (A_i, S_i) segment of $\mathcal{G}$. We simply say that $\mathcal{G}$ is a comprehensive Gröbner system of $\langle F\rangle$ over $\overline{K(u)}$ if $A_1 \cup \cdots \cup A_r = \left(\overline{K(u)}\right)^m$.

We have the following

Proposition Let $V_{\overline{\mathbb{C}(u)}}(E)$ be a non-empty stratum in $\overline{\mathbb{C}(u)}^m$ where $E \subset \mathbb{C}(u)[t]$. Set $E' = \{hq \in \mathbb{C}[u][t]|\forall h \in E,\ q$ is the least common multiple of all denominators of coefficients in $\mathbb{C}(u)$ of $h\}$ and $T = \{c_\alpha| \sum c_\alpha u^\alpha \in E', c_\alpha \in \mathbb{C}[t]\} \subset \mathbb{C}[t]$. Then, $V_{\mathbb{C}}(E) = V_{\mathbb{C}}(T)$ in $\mathbb{C}^m$. (Notice that $V_{\overline{\mathbb{C}(u)}}(E) \cap \mathbb{C}^m = V_{\mathbb{C}}(E)$.)

The above proposition allows us to design a deterministic method for computing Bertini type invariants for parametric cases.

Keywords
comprehensive Gröbner system, parametric ideal, Chern-Schewartz-MacPherson class

References

[1] P. Aluffi, Computing characteristic classes of projective schemes, *Jourrnal of Symbolic Computation* **35**, 3-19 (2003)

[2] D. J. Bates; J. D. Hauenstein; A. J. Sommese; C. W. Wampler *Bertini: Software for numerical algebraic geometry*, 2013, http://bertini.nd.edu/

[3] C. Harris; M. Helmer, Segre class computation and practical applications, *Math. Comp.* **89**, 465–491 (2020).

[4] M. Helmer, Algorithms to compute the topological Euler characteristics, Chern-Schwartz-MacPhersoon class of projective varieties, *J. Symbolic Comput.* **73**, 120–138 (2016).

[5] C. Jost, Computing characteristic classes and the topological Euler characteristics of complex projective schemes, *J. Softw. Algebra Geom.* **7**, 31-39 (2015).

[6] K. Nabeshima, Stability conditions of monomial bases and comprehensive Gröbner systems, *Lecture Notes in Comput. Sci.* **7442**, 248-259 (2012).

[7] M. H. Schwartz. *Classes de Chern des Ensembles Analytiques*. Hermann Paris, 2000

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *'Parametric Polynomial Systems"*

Imaginary projections: Complex versus real coefficients

Stephan Gardoll*[1]*, Thorsten Theobald*[2]*,
***Mahsa Sayyary Namin*[3]** [sayyary@math.uni-frankfurt.de]

[1,2,3] Goethe-Universität, Institut für Mathematik, Frankfurt am Main, Germany

Given a multivariate complex polynomial $p \in \mathbb{C}[z_1, \ldots, z_n]$, the imaginary projection $\mathcal{I}(p)$ of p is defined as the projection of the variety $\mathcal{V}(p)$ onto its imaginary part. We focus on studying the imaginary projection of complex polynomials and we state explicit results for certain families of them with arbitrarily large degree or dimension. Then, we restrict to complex conic sections and give a full characterization of their imaginary projections, which generalizes a classification for the case of real conics. That is, given a bivariate complex polynomial $p \in \mathbb{C}[z_1, z_2]$ of total degree two, we describe the number and the boundedness of the components in the complement of $\mathcal{I}(p)$ as well as their boundary curves and the spectrahedral structure of the components. We further show a realizability result for strictly convex complement components which is in sharp contrast to the case of real polynomials.

Keywords
Imaginary projection, Complex varieties, Convex algebraic geometry, Spectrahedron, Stable polynomial

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *‘Parametric Polynomial Systems”*

Generic Gröbner basis of a parametric ideal and its application to a comprehensive Gröbner system

Katsusuke Nabeshima[1] [nabeshima@rs.tus.ac.jp]

[1] Department of Applied Mathematics, Tokyo Univ. of Science, Kagurazaka, Tokyo, Japan

We introduce a new computational method for stability conditions of Gröbner bases and a new algorithm for computing comprehensive Gröbner systems.

The concepts of a comprehensive Gröbner basis and a comprehensive Gröbner system were introduced by V. Weispfenning [5] as a special basis of a parametric polynomial system and has been regarded as one of the new most important tools to study parametric systems. After 2001, by utilizing results of M. Kalkbrener [1], new effective algorithms have been introduced in A. Suzuki and Y. Sato [4]; D. Kapur et al. [2]; K. Nabeshima [3] for computing comprehensive Gröbner systems in a commutative polynomial ring.

We remark that since algorithms, that are presented in [2,3], are generalizations of the Suzuki-Sato algorithm [4], thus all the first steps of the algorithms, in [2,3,4], for computing comprehensive Gröbner systems are the same “computing a Gröbner basis in a polynomial ring over a polynomial ring”. Hence, the first steps also become the bottlenecks. Here we give a new method to become the substitute for computing the Gröbner basis.

We use the notation t as the abbreviation of m variables $t_1, \dots, t_m$ and the notation x as the abbreviation of n variables $x_1, \dots, x_n$. Let K and $\bar{K}$ be fields such that $\bar{K}$ is an algebraic closure field of K. Let $K[t][x]$ be a polynomial ring with coefficients in a polynomial ring $K[t]$. For $f_1, \dots, f_s \in K[x]$ (or $K[t][x]$), $\langle f_1, \dots, f_s \rangle = \{\sum_{i=1}^{s} h_i f_i | h_1, \dots, h_s \in K[x]$(or $K[t][x]$)$\}$. A symbol $\mathit{Term}(x)$ means the set of terms of x. Fix a term ordering $\succ$ on $\mathit{Term}(x)$. Let $f \in K[x]$ (or $f \in K[t][x]$), then $ht(f), ßhm(f)$ and $hc(f)$ denote the head term, head monomial and head coefficient of f i.e. $hm(f) = hc(f)ht(f)$. For $F \subset K[x]$ (or $F \subset K[t][x]$), $ht(F) = \{ht(f) | f \in F\}$. For $g_1, \dots, g_r \in K[t]$, $\mathbb{V}(g_1, \dots, g_r) \subset \bar{K}^m$ denote the affine variety of $g_1, \dots, g_r$, i.e. $\mathbb{V}(g_1, \dots, g_r) = \{\bar{t} \in \bar{K}^m \mid g_1(\bar{t}) = \cdots = g_r(\bar{t}) = 0\}$. In this talk, we use an algebraically constructible set that has a form $\mathbb{V}(f_1, \dots, f_\ell) \backslash \mathbb{V}(f'_1, \dots, f'_{\ell'}) \subset \bar{K}^m$ where $f_1, \dots, f_\ell, f'_1, \dots, f'_{\ell'} \in K[t]$. For $\bar{t} \in \bar{K}^m$, the canonical specialization homomorphism $\sigma_{\bar{t}} : K[t][x] \to \bar{K}[x]$ (or $K[t] \to \bar{K}$) is defined as the map that substitutes t by $\bar{t}$ in $f(t, x) \in K[t][x]$. The image $\sigma_{\bar{t}}$ of a set $F \subset K[t][x]$ is denoted by $\sigma_{\bar{t}}(F) = \{\sigma_{\bar{t}}(f) | f \in F\} \subset \bar{K}[x]$.

We adopt the following as a definition of comprehensive Gröbner system.

Definition 1. *Fix a term ordering $\succ$ on Term(x). Let $F \subset K[t][x]$, $\mathbb{A}_1, \dots, \mathbb{A}_r \subset \overline{K}^m$,*

$G_1, \ldots, G_r \subset K[t][x]$. *If a finite set* $\mathcal{G} = \{(\mathbb{A}_1, G_1), \ldots, (\mathbb{A}_r, G_r)\}$ *of pairs satisfies the properties such that*
- *for* $i \neq j$, $\mathbb{A}_i \cap \mathbb{A}_j = \emptyset$, *and*
- *for all* $\bar{t} \in \mathbb{A}_i$ *and* $g \in G_i$, $ht(g) = ht(\sigma_{\bar{t}}(g))$ *and* $\sigma_{\bar{t}}(G_i)$ *is a Gröbner basis of* $\langle \sigma_{\bar{t}}(F) \rangle$ *in* $\overline{K}[x]$,

then, $\mathcal{G}$ *is called a comprehensive Gröbner system (CGS) of* $\langle F \rangle$ *over* $\overline{K}$ *on* $\mathbb{A}_1 \cup \cdots \cup \mathbb{A}_r$. *We call a pair* $(\mathbb{A}_i, G_i)$ *segment of* $\mathcal{G}$. *We simply say that* $\mathcal{G}$ *is a comprehensive Gröbner system of* $\langle F \rangle$ *over* $\overline{K}$ *if* $\mathbb{A}_1 \cup \cdots \cup \mathbb{A}_r = \overline{K}^m$.

Let I be a monomial ideal in $K[x]$. Then, the minimal basis of I is written as $MB(I)$. In [3], Nabeshima gives the following theorem.

Theorem 2 (Nabeshima [3])**.** *Let* G *be a Gröbner basis of an ideal* $\langle F \rangle \subset K[t][x]$ *w.r.t. a term order* $\succ$ *on Term*(x) *and* $MB(\langle ht(G) \rangle) = \{m_1, \ldots, m_\ell\}$ *where* $F \subset K[t][x]$. *Suppose that* $G_i = \{f \in G | ht(f) = m_i\}$ *for each* $i \in \{1, \ldots, \ell\}$. *Then,* $\forall \bar{a} \in \bar{K}^m \backslash \bigcup_{i=1}^{\ell} \mathbb{V}(ht(G_i))$, $\sigma_{\bar{a}}(G_1 \cup G_2 \cup \cdots \cup G_\ell)$ *is a Gröbner basis of* $\langle \sigma_{\bar{a}}(F) \rangle$ *w.r.t.* $\succ$ *in* $\bar{K}[x]$.

In [2], Kapur-Sun-Wang give the following theorem.

Theorem 3 (Kapur-Sun-Wang [2])**.** *Using the same notation as in Theorem 2, let* $g_i \in G_i$ *and* $h_i = hc(g_i)$ *for each* $i \in \{1, \ldots, \ell\}$. *Then,* $\forall \bar{a} \in \bar{K}^m \backslash \mathbb{V}(h_1 \cdots h_\ell)$, $\sigma_{\bar{a}}(\{g_1, \ldots, g_\ell\}$ *is a minimal Gröbner basis of* $\langle \sigma_{\bar{a}}(F) \rangle$ *w.r.t.* $\succ$ *in* $\bar{K}[x]$.

The bottleneck of the both theorems above for getting the pairs $(\bar{K}^m \backslash \bigcup_{i=1}^{\ell} \mathbb{V}(ht(G_i)), \{G_1 \cup G_2 \cup \cdots \cup G_\ell\})$ or $(\bar{K}^m \backslash \mathbb{V}(h_1 \cdots h_\ell), \{g_1, \ldots, g_\ell\})$ is comptuing the Gröbner basis G of $\langle F \rangle$ in $K[t][x]$.

$\boxed{\textbf{Method 1}}$

Step 1: Computing a Gröbner basis G of $\langle F \rangle$ in $K[t][x]$.

Let $g = \sum_{i=1}^{r} c_{\alpha_i} x^{\alpha_i} \in K(t)[x]$ where $c_{\alpha_i} \in K(t)$, $\alpha_i \in \mathbb{N}^n$ and $K(t)$ is a field of rational functions. Then, $dlcm(g) = lcm(nd(c_{\alpha_1}), \ldots, nd(c_{\alpha_r}))$ where $nd(c_{\alpha_i})$ is the denominator of c_{α_i}.

The following theorem is a main result that is utilized in the new algorithm for computing comprehensive Gröbner systems.

Theorem 4. *Using the same notation as in Theorem 2, let* G' *be a reduced Gröbner basis of* $\langle F \rangle$ *w.r.t.* $\succ$ *in* $K(t)[x]$, $G'' = \{dlcm(g) \cdot g | g \in G'\}$, $h = \prod_{g \in G''} hc(g)$ *and* S *a reduced Gröbner basis of the ideal quotient* $\langle F \rangle : \langle G'' \rangle$ *w.r.t. a block term order with* $x \gg t$ *in* $K[t, x]$. *Then,*
(1) $S \cap K[t] \neq \emptyset$,
(2) for all $\bar{a} \in \bar{K}^m \backslash ((S \cap K[t]) \cup \mathbb{V}(h))$, $\sigma_{\bar{a}}(G')$ *is the reduced Gröbner basis of* $\langle \sigma_{\bar{a}}(F) \rangle$ *w.r.t.* $\succ$ *in* $\bar{K}[x]$.

In order to obtain the pair $(\bar{K}^m \backslash ((S \cap K[t]) \cup \mathbb{V}(h)), G')$, we have to compute a Gröbner basis G' of $\langle F \rangle$ in $K(t)[x]$ and a reduced Gröbner basis of the ideal quotient $\langle F \rangle : \langle G'' \rangle$.

$\boxed{\textbf{Method 2}}$

Step 1: Computing a reduced Gröbner basis G' of $\langle F \rangle$ in $K(t)[x]$.
Step 2: Computing the reduced Gröbner basis of the ideal quotient $\langle F \rangle : \langle G'' \rangle$.

In this talk, we report the comparison between Method 1 and Method 2, too.

Corollary 5. *Using the same notation as in Theorem 4, let $g \in S \cap K[t]$. Then, for all $\bar{a} \in \bar{K}^m \backslash \mathbb{V}(g \cdot h)$, $\sigma_{\bar{a}}(G')$ is the reduced Gröbner basis of $\langle \sigma_{\bar{a}}(F) \rangle$ w.r.t. $\succ$ in $\bar{K}[x]$.*

We also give a new algorithm for computing comprehensive Gröbner systems.

Keywords
comprehensive Gröbner system, stability of Gröbner basis, ideal quotient

References

[1] M. Kalkbrener, On the stability of Gröbner bases under specialization. *Journal of symbolic computation* **24**, 51–58 (1997).
[2] D. Kapur; Y. Sun; D. Wang, A new algorithm for computing comprehensive Gröbner systems. In *Proceedings of International Symposium on Symbolic and Algebraic Computation 2010*, pp. 29–36, ACM, 2010.
[3] K. Nabeshima, Stability conditions of monomial bases and comprehensive Gröbner systems. *Lecture Notes in Computer Science*, Vol. 7442, pp. 248–259, Springer, 2012.
[4] A. Suzuki; Y. Sato, A Simple algorithm to compute comprehensive Gröbner bases using Gröbner bases. In *Proceedings of International Symposium on Symbolic and Algebraic Computation 2006*, pp. 326–331. ACM, 2006.
[5] V. Weispfenning, Comprehensive Gröbner bases. *Journal of symbolic computation* **14**, 1–29 (1992).

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *'Parametric Polynomial Systems"*

Comprehensive Gröbner systems over finite fields

Ryoya Fukasaku[1]***, Yasuhiko Ikematsu***[2] [fukasaku@math.kyushu-u.ac.jp]

[1] Faculty of Mathematics, Kyushu University, Fukuoka, Japan
[2] Institute of Mathematics for Industry, Kyushu University, Fukuoka, Japan

A comprehensive Gröbner system (CGS) is a powerful tool for handling a parametric polynomial system, and plays a role as a Gröbner basis (GB) of a parametric polynomial ideal. By the algorithm introduced in [6] together with its improvements achieved in [3, 4, 5], it is now possible to build an efficient program for computing CGSs. So we have several its application programs. For example, a program for computing CGSs over an infinite field is applied to a real quantifier elimination program such as the one introduced in [2].

Since the theory of GBs allows us to analyze the algebraic structure of a given polynomial system, it is used in the security evaluation of multivariate public key cryptography (MPKC). In MPKC, a parametric polynomial system $\mathcal{P}$ over a finite field is constructed in some way, and a public key is generated by substituting random numbers r into the parameters of $\mathcal{P}$. Then a public key $\mathcal{P}(r)$ is a (non-parametric) polynomial system and varies with the value of r. The security of MPKC is analyzed by computing GBs of $\mathcal{P}(r)$ for some r. However, to our best knowledge, there has been no study to analyze the parametric polynomial system $\mathcal{P}$. We believe that we provide a new perspective in security evaluation of MPKC by computing a CGS of $\mathcal{P}$. Therefore, it is important to be able to compute CGSs over finite fields.

In this talk, we report on our program for computing CGSs over finite fields.

Keywords
Comprehensive Gröbner systems, Multivariate public key cryptography, Finite fields

References

[1] J. Ding; A. Petzoldt; D.S. Schmidt, Multivariate Public Key Cryptosystems, Second Edition, Springer, 2020.
[2] R. Fukasaku; H. Iwane; Y. Sato, Real Quantifier Elimination by Computation of Comprehensive Gröbner Systems. In *Proceedings of International Symposium on Symbolic and Algebraic Computation 2015*, pp. 173–180, ACM, 2015.
[3] D. Kapur; Y. Sun; D. Wang, A New Algorithm for Computing Comprehensive Gröbner Systems. In *Proceedings of International Symposium on Symbolic and Algebraic Computation 2010*, pp. 29–36, ACM, 2010.
[4] Y. Kurata, Improving Suzuki-Sato's CGS Algorithm by Using Stability of Gröbner Bases and Basic Manipulations for Efficient Implementation. *Communications of the Japan*

Society for Symbolic and Algebraic Computation, Vol. 1, pp. 39–66, JSSAC, 2011.
[5] K. NABESHIMA, Stability Conditions of Monomial Bases and Comprehensive Gröbner systems. *Lecture Notes in Computer Science*, Vol. 7442, pp. 248–259, Springer, 2012.
[6] A. SUZUKI; Y. SATO, A Simple Algorithm to Compute Comprehensive Gröbner Bases Using Gröbner Bases. In *Proceedings of International Symposium on Symbolic and Algebraic Computation 2006*, pp. 326–331. ACM, 2006.

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *‘Parametric Polynomial Systems”*

Implementation report on parametric absolute factorization of multi-variate polynomials

Kazuhiro Yokoyama[1] [kazuhiro@rikkyo.ac.jp]

[1] Rikkyo University, Tokyo 171-8501, Japan.

This is a continuation of the author's paper [6] where a computational strategy for *parametric polynomial ideal decomposition*, where a parametric polynomial ideal means an ideal generated by polynomials with parametric coefficients. In [6], the notion of the stability of *ideal structures*, such as radicalness and certain primality, is given by using the notion of so-called *comprehensive Gröbner bases*. Moreover, computational methods are proposed for classifying the values of parameters for such stable structures of ideals . (As references, see [1, 5] for the stability of Gröbner basis, [2, 3, 4] for computational methods of comprehensive Gröbner bases of polynomial ideals.)

Actually, for a parametric polynomial ideal, its radical computation and prime/primary decomposition, can be described uniformly and we may call them *parametric decomposition*. But, the practicality of such parametric decomposition or its efficient realization on real computer is not investigated yet.

For prime/primary decomposition, the most important and difficult part is to classify the values of parameters for the stable primality of ideals as semi-algebraic sets. And such decomposition is certainly reduced to absolutely irreducible factorization of polynomials with parametric coefficient. (Here we call it parametric factorization, in short.) Also in [6], a naive method is given for handling parametric factorization. We note that absolute irreducibility is necessary for our classification on parameter values in semi-algebraic sets. Because, irreducibility condition on parameters may not be semi-algebraic in non-algebraic closure fields. Also, as univariate polynomials can be decomposed into their linear factors in algebraic closed fields, we consider multi-variate polynomials.

In this talk, we report our current status of realization of parametric factorization based on the naive method, and give some practical improvement.

Keywords
comprehensive Gröbner system, primary decomposition

References

[1] M. Kalkbrener, On the stability of Gröbner bases under specialization. *Journal of symbolic computation* **24**, 51–58 (1997).

[2] A. Montes, A new algorithm for discussing Gröbner bases with parameters. *Journal of symbolic computation* **33**, 183 - 208. (2002).

[3] K. NABESHIMA, A speed-up of the algorithm for computing comprehensive Gröbner systems. *In Proceedings of ISSAC 2007*, pp. 183–208, ACM, 2007.

[4] A. SUZUKI; Y. SATO, A Simple Algorithm to compute comprehensive Gröbner bases using Gröbner bases. In *Proceedings of International Symposium on Symbolic and Algebraic Computation 2006*, pp. 326–331. ACM, 2006.

[5] V. WEISPFENNING, Comprehensive Gröbner bases. *Journal of symbolic computation* **14**, 1–29 (1992).

[6] K. YOKOYAMA, Stability of Parametric Decomposition. *LNCS*, Vol. 4151, pp. 391–402, Springer, 2006.

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *‘Parametric Polynomial Systems”*

Simplification of comprehesive Gröbner systems using disequalities

Yosuke Sato [ysato@rs.tus.ac.jp]

Department of Applied Mathematics, Tokyo University of Science, Tokyo, Japan

A comprehensive Gröbner system (CGS) is a powerful tool for handling parametric polynomial systems. Its first practical computation algorithm was introduced in [6]. With improvements of the subsequent works such as [3,4,5], we now have several its application programs such as the one introduced in [2].

It seems that a basic framework of its practical computation algorithm was established by the work of [5] at least from a theoretical point of view, however, there still remain many important issues concerning its efficient implementation. We have developed several techniques which improve the existing implementations of CGS. In the talk [7] of the last ACA2021, we reported that our techniques are quite effective through our implementation in SageMath [1]. Since our work was on going at that point, however, several important theoretical issues were still remaied open.

In the talk, we introduce several concepts concerning simplification of CGS and settle the above open problems.

Keywords
Comprehensive Gröbner System, SageMath

References

[1] *SageMath*, A free open-source mathematics software system licensed under the GPL. https://www.sagemath.org/
[2] R. FUKASAKU; H. IWANE; Y. SATO, *Real Quantifier Elimination by Computation of Comprehensive Gröbner Systems.* Proceedings of International Symposium on Symbolic and Algebraic Computation, pp. 173–180, ACM, 2015.
[3] D. KAPUR; Y. SUN; D. WANG, *A New Algorithm for Computing Comprehensive Gröbner Systems.* Proceedings of International Symposium on Symbolic and Algebraic Computation, pp. 29–36, ACM, 2010.
[4] Y. KURATA, *Improving Suzuki-Sato's CGS Algorithm by Using Stability of Gröbner Bases and Basic Manipulations for Efficient Implementation.*, Communications of the Japan Society for Symbolic and Algebraic Computation, Vol. 1, pp. 39–66, JSSAC, 2011.
[5] K. NABESHIMA, *Stability Conditions of Monomial Bases and Comprehensive Gröbner systems.*, Lecture Notes in Computer Science, Vol. 7442, pp. 248–259, Springer, 2012.

[6] A. SUZUKI; Y. SATO, *A Simple Algorithm to Compute Comprehensive Gröbner Bases Using Gröbner Bases.* Proceedings of International Symposium on Symbolic and Algebraic Computation, pp. 326–331, ACM, 2006.

[7] M. TANIWAKI; Y. SATO, *Some tips on the implementation of CGS in SageMath.* Presented in ACA2021, Virtual Online, July 23-27, 2021.

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2021
Session on *“q-Analogues in Combinatorics: Matroids, Designs and Codes”*

An alternative for the q-matroid axiom (I4)

Michela Ceria[1]**, *Relinde Jurrius***[2] [rpmj.jurrius@mindef.nl]

[1] Politectico di Bari, Italy
[2] Netherlands Defence Academy, The Netherlands

A q-matroid can be defined as a pair $(E, \mathcal{I})$ where E is a finite dimensional space and $\mathcal{I}$ is a collection of independent spaces, satisfying

(I1) $\mathcal{I} \neq \emptyset$.

(I2) If $J \in \mathcal{I}$ and $I \subseteq J$, then $I \in \mathcal{I}$.

(I3) If $I, J \in \mathcal{I}$ with $\dim I < \dim J$, then there is some 1-dimensional subspace $x \subseteq J$, $x \nsubseteq I$ with $I + x \in \mathcal{I}$.

(I4) Let $A, B \subseteq E$ and let I, J be maximal independent subspaces of A and B, respectively. Then there is a maximal independent subspace of $A + B$ that is contained in $I + J$.

Contrary to the classical case, the axiom (I4) is really needed to define a q-matroid [1]. Apart from the fact that it makes the proof of q-cryptomorphisms work [2], it is not straightforward to see where this axiom comes from. In this talk we will zoom in on the q-matroid axioms (I3) and (I4), and propose an alternative version of (I3). This new axiom can also be seen as a q-analogue of the axiom (I3) for classical matroids, and moreover it make the axiom (I4) obsolete.

Keywords
q-analogue, q-matroid, cryptomorphism

References

[1] R. JURRIUS; R. PELLIKAAN, Defining the q-analogue of a matroid. *Electronic Journal of Combinatorics* **25**, P3.2 (2018).
[2] E. BYRNE; M. CERIA; R. JURRIUS, Constructions of new q-cryptomorphisms. *Journal of Combinatorial Theory, Series B* **153**, 149–194 (2022).

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2021
Session on *“q-Analogues in Combinatorics: Matroids, Designs and Codes”*

The direct sum of q-matroids

Michela Ceria[1]**,*Relinde Jurrius***[2] [michela.ceria@poliba.it]

[1] Department of Mechanics, Mathematics and Management, Politecnico di Bari, Italy [2] Faculty of Military Sciences, Netherlands Defence Academy, The Netherlands

For classical matroids, the direct sum is one of the most straightforward methods to make a new matroid out of existing ones.

In this talk we will define a direct sum for q-matroids, the q-analogue of matroids. This is a lot less straightforward than in the classical case, and we will see the reasons of that.

With the use of q-polymatroids and the q-analogue of matroid union we come to a definition of the direct sum of q-matroids.

As a motivation for this definition, we show it has some desirable properties.

This talk is based on the paper [1].

References

[1] M. Ceria, R. Jurrius, *The direct sum of q-matroids*, arXiv:2109.13637v3 [math.CO]

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2021
Session on *"q-Analogues in Combinatorics: Matroids, Designs and Codes"*

q-Matroids and Rank-Metric Codes

Gianira N. Alfarano[1], ***Eimear Byrne***[2] [gianiranicoletta.alfarano@math.uzh.ch]

[1] Institute of Mathematics, University of Zurich, Zurich,
Switzerland
[2] School of Mathematics and Statistics, University College Dublin,
Belfield, Ireland

In classical combinatorics, matroids generalize the notion of linear independence of vectors over a field. In this talk, we will introduce the concept of $\mathbb{F}_{q^m}$-independence of $\mathbb{F}_q$-spaces and we show that q-matroids generalize this notion. As a consequence, the independent spaces of a representable q-matroid will be defined as the $\mathbb{F}_{q^m}$-independent subspaces of the q-system associated to an $\mathbb{F}_{q^m}$-linear rank-metric code. Moreover, we will further investigate the link between codes and matroids.

This talk is based on the paper [1].

Keywords
q-matroids; rank-metric codes; independence.

References

[1] G. N. ALFARANO, E. BYRNE., *The Cyclic Flats of q-Matroids.*. submitted, 2022.

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2021
Session on *"q-Analogues in Combinatorics: Matroids, Designs and Codes"*

A Geometric Characterization of Near MRD Codes

Alessandro Neri[1] [alessandro.neri@mis.mpg.de]

[1] Max Planck Institute for Mathematics in the Sciences, Leipzig, Germany

The notion of q-system has been introduced in [4] in order to give a geometric interpretation for rank-metric codes which are linear over an extension field $\mathbb{F}_{q^m}$. An $[n,k]_{q^m/q}$ system (or simply q-system) is an $\mathbb{F}_q$-subspace $\mathcal{U} \subseteq \mathbb{F}_{q^m}^k$ of dimension n, which is not contained in any $\mathbb{F}_{q^m}$-hyperplane. It was shown that to a k-dimensional $\mathbb{F}_{q^m}$-linear rank-metric code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ one can associate – up to equivalence – the $[n,k]_{q^m/q}$ system $\mathcal{U}$ given by the $\mathbb{F}_q$-span of the columns of a generator matrix $G \in \mathbb{F}_{q^m}^{k\times n}$ for $\mathcal{C}$.

From a combinatorial point of view, the q-system captures the geometry of the rank supports of a rank-metric code $\mathcal{C}$. It was indeed shown in [3] that for any nonzero $u \in \mathbb{F}_{q^m}^k$, one has

$$\mathrm{supp}(uG)^\perp = \psi_G^{-1}(\mathcal{U} \cap u^\perp),$$

where

$$\begin{array}{rcl} \psi_G : \mathbb{F}_q^n & \longrightarrow & \mathcal{U} \\ \lambda & \longmapsto & \lambda G^\top. \end{array}$$

This implies that the rank weights of the codewords of $\mathcal{C}$ are fully determined by the intersections of $\mathbb{F}_{q^m}$-hyperplanes of $\mathbb{F}_{q^m}^k$ with the q-system $\mathcal{U}$. Furthermore, one also can determine the i-th generalized rank weight of $\mathcal{C}$ by intersecting $\mathcal{U}$ with $(k-i)$-dimensional $\mathbb{F}_{q^m}$-subspaces; see [4].

In this talk, we will discuss the interplay between the generalized rank weights of a rank-metric code $\mathcal{C}$ and the evasiveness properties of the associated q-system $\mathcal{U}$. Evasiveness is a concept originally introduced for explicit constructions of Ramsey graphs and of list decodable codes with optimal rate. This notion gives a measure on the intersection of a q-system with r-dimensional $\mathbb{F}_{q^m}$-subspaces of $\mathbb{F}_{q^m}^k$. Formally, a q-system $\mathcal{U}$ is (h,r)-evasive if $\dim_{\mathbb{F}_q}(\mathcal{U} \cap H) \leq r$ for every h-dimensional $\mathbb{F}_{q^m}$-subspace H of $\mathbb{F}_{q^m}^k$.

We will see how geometric results can be helpful to determine features of rank-metric codes and, vice versa, how known properties of the generalized rank weights can be helpful to determine evasiveness of the associated q-system. We will conclude by giving a geometric characterization of near MRD codes, and bounds on their maximal length obtained in [2], settling an analogue of the main conjecture on near MDS codes posed in [1].

Keywords
rank-metric codes, q-systems, evasive subspaces, near MRD codes, generalized rank weights.

References

[1] I. LANDJEV, IVAN, A. ROUSSEVA, The main conjecture for near-MDS codes, In *WCC2015 - 9th International Workshop on Coding and Cryptography*, 2015.

[2] G. MARINO, A. NERI, R. TROMBETTI, *Evasive subspaces, generalized rank weights and near MRD codes*. preprint, arXiv:2204.11791, (2022).

[3] A. NERI, P. SANTONASTASO, F. ZULLO, *The geometry of one-weight codes in the sum-rank metric*. preprint, arXiv:2112.04989, (2021).

[4] T. RANDRIANARISOA, A geometric approach to rank metric codes and a classification of constant weight codes. *Designs, Codes and Cryptography*, **88**, 1331–1348 (2020).

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2021
Session on *“q-Analogues in Combinatorics: Matroids, Designs and Codes”*

q-analog of Sidon sets and linear sets

Vito Napolitano, Olga Polverino, Paolo Santonastaso, Ferdinando Zullo[1] [ferdinando.zullo@unicampania.it]

[1] Dipartimento di Matematica e Fisica, Università degli Studi della Campania “Luigi Vanvitelli”, Caserta, Italy

The q-analog of Sidon sets is known as Sidon spaces, introduced by Bachoc, Serra and Zémor in 2017 in [1] in relation with the linear analogue of Vosper's Theorem. An $\mathbb{F}_q$-subspace U of $\mathbb{F}_{q^n}$ is called a **Sidon space** if the product of any two elements of U has a unique factorization over U, up to multiplying by some elements in $\mathbb{F}_q$. More precisely, U is a Sidon space if for all nonzero $a, b, c, d \in U$, if $ab = cd$, then

$$\{a\mathbb{F}_q, b\mathbb{F}_q\} = \{c\mathbb{F}_q, d\mathbb{F}_q\},$$

where if $e \in \mathbb{F}_{q^n}$ then $e\mathbb{F}_q = \{e\lambda \colon \lambda \in \mathbb{F}_q\}$. In this talk we will see an application of Sidon spaces to linear sets. Linear sets have been deeply studied and there is still a massive attention on them, as they have been used to construct and classify several objects. In this talk we will deal with linear sets of **minimum size** in $\mathrm{PG}(1, q^n)$ [2]. Examples of these linear sets have been found by Lunardon and Polverino in 2000 and, more recently, by Jena and Van de Voorde in [3]. However, classification results for minimum size linear sets of rank k are known only for $k \leq 5$. In this talk we will provide classification results for linear sets of minimum size when n is prime, answering to a question in [3]. Then we construct new examples when n is not prime. The main tool relies on studying pairs of subspaces (*critical pairs*) attaining the equality in the linear analogue of Cauchy-Davenport's theorem. The talk is based on the paper arXiv:2201.02003.

Keywords
Sidon space, linear set, critical pair

References

[1] C. BACHOC, O. SERRA, G. ZÉMOR, An analogue of Vosper's theorem for extension fields, *Math. Proc. Cambridge Philos. Soc.* **163**(3):423–452, 2017.
[2] J. DE BEULE, G. VAN DE VOORDE, The minimum size of a linear set, *Journal of Combinatorial Theory, Series A*, **164**:109–124, 2019.
[3] D. JENA, G. VAN DE VOORDE, On linear sets of minimum size, *Discrete Mathematics*, **344**(3):112230, 2021.

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2021
Session on *"q-Analogues in Combinatorics: Matroids, Designs and Codes"*

Independent Spaces of q-Polymatroids

Heide Gluesing-Luerssen[1], ***Benjamin Jany***[2] [heide.gl@uky.edu]

[1,2] University of Kentucky, Department of Mathematics, 40506 Lexington, KY, USA.

It is well known that $\mathbb{F}_{q^m}$-linear rank-metric codes in $\mathbb{F}_{q^m}^n$ give rise to q-matroids [5], whereas the more general $\mathbb{F}_q$-linear rank-metric codes in $\mathbb{F}_q^{n\times m}$ lead to q-polymatroids [4]. The latter differ from q-matroids in that the rank function may assume rational values. This seemingly slight generality has vast consequences for the theory of q-polymatroids. While for q-matroids a variety of cryptomorphic descriptions have been established [1], little is known so far for q-polymatroids.

In this talk we introduce, for any common denominator μ of the rank function, a notion of μ-independent spaces for q-polymatroids. With the aid of an auxiliary q-matroid, we establish properties of the collection of independent spaces similar to those for q-matroids. It follows that the entire q-polymatroid is fully determined by the collection of μ-independent spaces along with the rank values on those spaces. All of this can be used to derive a cryptomorphism for q-polymatroids based on independent spaces along with a rank function defined on those spaces. Examples show that no such cryptomorphism is possible using, for instance, bases, dependent spaces, or circuits. The talk is based on the material in [2, 3].

Keywords
q-(poly)matroids, independent spaces, cryptomorphisms, rank-metric codes.

References

[1] E. Byrne; M. Ceria; R. Jurrius. Constructions of new q-cryptomorphisms. *J. Comb. Theory. Ser. B*. 153:149–194, 2022.

[2] H. Gluesing-Luerssen; Benjamin Jany. q-Polymatroids and their Relation to Rank-Metric Codes. *J. Algebraic Combin.* DOI 10.1007/s10801-022-01129-y. To appear.

[3] H. Gluesing-Luerssen; Benjamin Jany. Independent Spaces of q-Polymatroids. *Algebraic Combinatorics*. To appear.

[4] E. Gorla; R. Jurrius; H. López; A. Ravagnani. Rank-Metric Codes and q-Polymatroids. *J. Algebraic Combin.*, 52:1–19, 2020.

[5] R. Jurrius; R. Pellikaan. Defining the q-Analogue of a Matroid. *Electron. J. Combin.* 25: P3.2, 2018.

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2021
Session on *"q-Analogues in Combinatorics: Matroids, Designs and Codes"*

Categories of q-Matroids

Benjamin Jany[1], ***Heide Gluesing-Luerssen***[2] [benjamin.jany@uky.edu]

[1,2] University of Kentucky, Department of Mathematics. 40506, Lexington, KY, USA.

In recent years, q-matroids, the q-analogue of a matroid, have been a focus of research in coding theory because of their usefulness in studying rank metric codes. Because of their q-analogue nature, it has been of interest to find which matroidal notions and properties generalize to q-matroids. Similarly to matroids, one can define weak and strong maps between q-matroids which respectively respect the rank and flat structure. These maps can be used to define categories of q-matroids, allowing to study q-matroids from a more category theory approach. Taking this approach helps in finding similarities and differences between the structure of matroids and that of q-matroids. In this talk, we will introduce the notions of weak and strong maps for matroids and q-matroids. We will then show the existence of a functor from categories of q-matroids to categories of matroids given by projectivizing the groundspace of a q-matroid. Finally we will discuss differences between the two type of categories by showing that unlike for categories of matroids, a coproduct may not always exist in the category of q-matroids with strong maps but does always exist when the morphisms are linear weak maps.

Keywords
q-matroid, matroid, weak map, strong map, coproduct

References

[1] H. GLUESING-LUERSSEN; B. JANY, *Coproducts in Categories of* q*-Matroids*, arXiv:2111.09723v2 , 2022.

[2] B. JANY, *The Projectivization Matroid of a q-Matroid*, arXiv:2204.01232v2, 2022.

[3] M. CERIA; R. JURRIUS, *The direct sum of q-matroids*, arXiv:210913637v3, 2022.

[4] H. CRAPO; G.-C. ROTA, *On the Foundations of Combinatorial Theory: Combinatorial Geometries*. MIT Press, 1970.

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2021
Session on *"q-Analogues in Combinatorics: Matroids, Designs and Codes"*

A q-analogue of Critical Theorem for polymatroids

Koji Imamura[1]***, Keisuke Shiromoto***[1] [211d9321@kumamoto-u.ac.jp]

[1] Department of Mathematics and Engineering, Kumamoto University, Kumamoto, Japan

The Critical Problem posed by H. Crapo and G.-C. Rota is one of the significant problems in matroid theory. It is the problem for finding the maximum dimension of a subspace that contains no member of a fixed subset S of $\mathbb{F}_q^k$. The problem is also equivalent to determining the critical exponent of the associated matroid, and J.P.S. Kung [4] gave an upper bound on it. The Critical Theorem, which provides another approach to the Critical Problem, has been interpreted in terms of code theory in [1]. After that, Kung's results were generalized to linear codes over finite fields in [2], and then extended to the case of finite chain rings [3]. In this talk, to formulate the Critical Problem for a q-analogue of polymatroids which was introduced in [5], we will define the critical exponent of them as an analogue of that of representable matroids. Consequently, we will generalize the Critical Theorem and Kung's upper bound to a q-analogue of polymatroids by associating them with Delsarte rank-metric codes.

Keywords
Delsarte Rank-Metric Codes, Critical Problem, Polymatroids

References

[1] T. BRITZ, Extensions of the critical theorem. *Discrete Math.* **volume**(305), 55–73 (2005).

[2] T. BRITZ; K. SHIROMOTO, On the covering dimension of a linear code. *IEEE Trans. Inf. Theory* **volume**(56) 4350–4358 (2010).

[3] K. IMAMURA; K. SHIROMOTO, Critical Problem for codes over finite chain rings. *Finite Fields Their Appl.* **volume**(76), 101900 (2021).

[4] J.P.S. KUNG, Critical problems, in *Matroid Theory*, Seattle, WA, 1995, *Contemporary Mathematics*, **volume**(197), American Mathematical Society, Providence RI, 1–127 (1996).

[5] K. SHIROMOTO, Codes with the rank metric and matroids, *Des. Codes Cryptogr.*, **volume**(87), 1765–1776 (2019).

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2021
Session on *"q-Analogues in Combinatorics: Matroids, Designs and Codes"*

Shellability and homology of q-complexes associated to q-matroids

Sudhir R. Ghorpade[1] [srg@math.iitb.ac.in]

[1]Department of Mathematics, Indian Institute of Technology Bombay, Powai, Mumbai 400076, India

The notion of a q-complex is a straightforward generalization of the classical notion of an abstract simplicial complex, and it goes back at least to Rota (1971). Shellability for a q-complex was defined by Alder (2010), thus providing a q-analogue of a property of simplicial complexes that has proved to be immensely useful in algebraic combinatorics and combinatorial topology. The study of q-matroids goes back to Crapo (1964) and has seen a resurgence in the recent past owing to the work of Jurrius and Pellikaan (2018) where the relevance of q-matroids for the study of rank metric codes was shown. It thus seems natural to ask for a q-analogue of the classical result that simplicial complexes formed by independent subsets of a matroid are shellable.

In this talk, we will begin by outlining a recent work [1] where it is shown that any q-matroid complex, i.e., any q-complex formed by the independent subspaces of a q-matroid, is always shellable. Furthermore, we outline the results in [1] which determine the homology of several (but not all) q-matroid complexes. We will then explain some parts of a newer work [2] where more complete results on the homology of q-matroid complexes as well as their order complexes are obtained and also it is shown that the order complex of a q-matroid complex is shellable.

This is a joint work [1] with Rakhi Pratihar and Tovohery Randrianarisoa, and also a joint work [2] with Rakhi Pratihar, Tovohery Randrianarisoa, Glen Wilson, and Hugues Verdure.

Keywords
q-complex, q-matroid, shellability, homology, order complex.

References

[1] S. R. GHORPADE; R. PRATIHAR; T. H. RANDRIANARISOA, Shellability and homology of q-complexes and q-matroids, *Journal of Algebraic Combinatorics*, 2022, 28 pp. (doi:10.1007/s10801-022-01150-1).

[2] S. R. GHORPADE; R. PRATIHAR; T. H. RANDRIANARISOA; G. WILSON; H. VERDURE, Homotopy type of shellable q-complexes and their homology groups, *in preparation*.

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2021
Session on *"q-Analogues in Combinatorics: Matroids, Designs and Codes"*

Generalized rank weights and Betti numbers

Rakhi Pratihar[1] [pratihar.rakhi@gmail.com]

[1]Department of Mathematics, Indraprastha Institute of Information Technology Delhi, India

In 2013, Johnsen and Verdure showed how one can associate a fine set of invariants, called Betti numbers to linear codes (with the Hamming metric) and more generally, to matroids. They also showed that the Betti numbers of a linear code determine its generalized Hamming weights. We consider the question of defining an analogous notion of Betti numbers for Gabidulin rank-metric codes, and more generally, q-matroids, in such a way that the generalized rank weights are determined by these Betti numbers.

Motivated partly by a topological approach to the above question, it was shown in a recent work [1] that q-complexes corresponding to q-matroids are shellable and moreover, their singular homology can be determined in several cases. But to relate the singular homology with the generalized rank weights, one needs to know how the singular homology is related to the nullity of q-cycles of the concerned q-matroid. This is far from clear.

In this talk, I will present a combinatorial approach to answer the question raised above. I will show how the generalized rank weights and the weight spectra of Gabidulin rank-metric codes can be determined from the Betti numbers of a classical matroid corresponding to the q-matroid associated to the code. I will also briefly discuss how the singular homology mentioned above are not related to the Betti numbers the way it does in the classical case.

This talk is mostly based on a joint work [2] with Trygve Johnsen and Hugues Verdure. **Keywords**

Rank-metric codes, q-Matroids, q-Cycles, Singular Homology, Betti numbers, Möbius function

References

[1] S. R. Ghorpade; R. Pratihar; T. H. Randrianarisoa, Shellability and Homology of q-Complexes and q-Matroids, *Journal of Algebraic Combinatorics*, 2022, (doi:10.1007/s10801-022-01150-1).
[2] T. Johnsen; R. Pratihar; H. Verdure, Weight Spectra of Gabidulin Rank-Metric Codes and Betti Numbers, *São Paulo Journal of Mathematical Sciences*, 2022, (doi:10.1007/s40863-022-00314-y).

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey | August 15-19, 2022
Session on *"Computer Algebra Applications in the Life Sciences"*

Detecting and precluding toricity in reaction network theory

Elisenda Feliu[1]**, *Oskar Henriksson***[1] [oskar.henriksson@math.ku.dk]

[1] Department of Mathematical Sciences, University of Copenhagen, Copenhagen, Denmark

One of the big themes in algebraic reaction network theory is the attempt to understand the qualitative properties of the steady states of a network under the assumption of mass action kinetics. Examples of such properties include stability, absolute concentration robustness and multistationarity. Some of these properties are easier to study when the positive steady state variety is known to be toric, in the sense that it admits a monomial parameterization, and it is therefore desirable to find criteria for when such parameterizations exist.

Previous work in this direction has focused on deficiency theory, binomiality of the steady state ideal, and quantifier elimination methods. In this talk, I will present new conditions for asserting and precluding toricity, based on the polyhedral geometry of the flux cone, as well as previously known results on injectivity of monomial maps restricted to linear subspaces. These conditions allow us to quickly deduce information about the potential for toricity and multistationarity for moderately sized networks, which we demonstrate by testing our methods on networks from the database ODEbase.

Keywords
Reaction networks, Mass-action kinetics, Flux cone, Toric varieties, Multistationarity.

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey | August 15-19, 2022
Session on *“Computer Algebra Applications in the Life Sciences”*

Estimating Genomic Periodicities

Daniel Lichtblau [danl@wolfram.com]

Kernel Technology group at Wolfram Research, US

Determining the periodicity of phenomena from unevenly sampled data is an important problem in several fields. This is particularly a challenge when the data is not numeric, as is the case with genomic sequences. I will show two approaches to this task that can be applied directly to such strings, that is, without first converting to numeric values. One is related to the Fourier Transform while the other is an application of simultaneous Diophantine approximation. Despite their very different origins, they share a surprising feature: both involve binning along the “*wrong*” axis. I will illustrate these methods on a reference yeast sequence. One gives a notable improvement over prior studies. Time permitting I may also show an application with the SARS-CoV-2 genome.

Keywords
Genomic periodicities, Fourier transform, Diophantine approximation

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey | August 15-19, 2022
Session on *"Computer Algebra Applications in the Life Sciences"*

Are generic bifurcations always generic on chemical reaction networks?

Nicola Vassena [nicola.vassena@fu-berlin.de]

Institute of Mathematics, Free University Berlin, Berlin, Germany

In dynamical systems, bifurcation analysis is a powerful tool to detect parameter areas that show important features such as multistationarity and oscillations. Saddle-node, Hopf, and Takens-Bogdanov bifurcations are examples of generic bifurcations, i.e., happening generically in the set of parametric vector fields with an equilibrium whose Jacobian satisfies some simple spectral conditions. Since any bifurcation can be perturbed to a generic bifurcation, we shall always expect generic bifurcations in applications, unless there is "something special" about the formulation of the problem that strongly restricts the context.

For vector fields arising from chemical reaction networks, we may choose with quite a freedom the nonlinearities (kinetics) governing the reaction rates, but the network structure is typically considered fixed. In this talk we address a natural question: Can the algebraic structure of the network itself be "something special" preventing generic bifurcations from occurring? In other words, do such generic bifurcations always happen generically in the set of vector fields with a fixed network structure? Focusing on saddle-node bifurcation, we discuss a few (counter)examples.

Keywords
Chemical Reaction Networks, Bifurcation analysis, Genericity

References

[1] N. VASSENA, Structural obstruction to the simplicity of the eigenvalue zero in chemical reaction networks. *arXiv:2205.12655*. Submitted. (2022)

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey | August 15-19, 2022
Session on *“Computer Algebra Applications in the Life Sciences”*

Stability analysis and Hopf bifurcations in a tumor growth model

***Dániel András Drexler* [1], *Ilona Nagy*[2] *Valery G. Romanovski*[3,4]**
[valerij.romanovskij@um.si]

[1] Óbuda University, Physiological Controls Research Center, Budapest, Hungary
[2] Department of Analysis, Institute of Mathematics, Budapest University of Technology and Economics, Budapest, Hungary
[3] Faculty of Electrical Engineering and Computer Science and Faculty of Natural Science and Mathematics, University of Maribor, Maribor, Slovenia
[4] Center for Applied Mathematics and Theoretical Physics, University of Maribor, Maribor, Slovenia

We carry out qualitative analysis of a fourth-order tumor growth control model using ordinary differential equations. We show that the system has one positive equilibrium point and its stability is independent of the feedback gain. Using a Lyapunov functions method we prove that there exist realistic parameter values for which the systems admits limit cycle oscillations due to a supercritical Hopf bifurcation [1]. The time evolution of the state variables is also represented. The study is a continuation of the analysis performed in [2].

Keywords
Tumor therapy, Cancer therapy, Tumor control, Singular point, Bifurcation, Limit cycle

References

[1] D. A. DREXLER, I. NAGY, AND V. G. ROMANOVSKI, Stability analysis of the singular points and Hopf bifurcations of a tumor growth control model (Mathematica notebook), (2022), http://math.bme.hu/~nagyi/Mathematica_notebooks/index.html.
[2] D. A. DREXLER, I. NAGY, AND V. G. ROMANOVSKI, Bifurcations in a closed-loop model of tumor growth control. In *Proceedings of the 21th IEEE International Symposium on Computational Intelligence and Informatics*, 329–334, Budapest, 2021.

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey | August 15-19, 2022
Session on *"Computer Algebra Applications in the Life Sciences"*

The shape of the parameter region of multistationarity in reaction networks

Elisenda Feliu[1], ***Máté L. Telek***[1] [mlt@math.ku.dk]

[1] Department of Mathematical Sciences, University of Copenhagen, Copenhagen, Denmark

Despite recent developments, describing the set of parameters that enable multistationarity in a chemical reaction network is a challenging problem. In this talk, I will present a new algorithm that permits insights into the shape of the parameter region of multistationarity, in particular on its connectivity. The method is based on the observation that, under some assumptions on the network, one can decide the connectivity of the parameter region of multistationarity, based on the connectivity of the preimage of the negative real line under a multivariate signomial function. The later problem can be addressed by considering the geometry of the Newton Polytope of the signomial function.

I will give several examples of reaction networks where our algorithm can be applied. In particular, we show that the parameter region of multistationarity of the sequential and distributive phosphorylation cycle with two or three sites is connected.

Keywords
Reaction networks, multistationarity, polyhedral geometry

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey | August 15-19, 2022
Session on *"Computer Algebra Applications in the Life Sciences"*

Disaster Incident Analysis via Algebra Stories

Berina Celic[1]***, Bernhard Garn***[1]***, Dimitris E. Simos***[1]
[{bcelic,bgarn,dsimos}@sba-research.org]

[1] SBA Research, Vienna, Austria

Natural disasters increasingly threaten the safety of modern humanity and a trend of more and more frequent natural disasters have been observed in recent decades [1]. Therefore, it is very important to analyze past disasters or crises that have happened for the purpose of their prevention or damage reduction in the future. One of the main sources for analyzing former disaster response actions are the official reports of emergency services and governmental case studies [2]. These documents often contain detailed descriptions of the timeline of disasters in natural language and their automated large-scale analysis can be done by modern *natural language processing* (NLP) [3] software solutions.

In this talk, we enhance the analysis capabilities of former disasters by integrating computer algebra techniques into this process and present the design of an automated information ex-traction framework for post-disaster case study reports based on NLP. In particular, we will showcase how to interpret the extraction of mathematical data and information from such case studies by NLP as an *algebra story problem* [4], thereby greatly increasing the data ex-traction capabilities. We will illustrate what kind of embedded mathematical information can be extracted from disaster reports with several examples. Further, the extracted information can be used as an input for a *Structured Scientific Knowledge Representation* (SSKR) object for further analysis [5], with one important use case being disaster scenario generation for evaluating different disaster response management strategies.

Keywords
Natural disasters, Disaster management, Natural language processing, Computer algebra, Knowledge Representation.

References

[1] D. Guha-Sapir, *EM-DAT: the emergency events database*. Euniversité catholique de louvain (UCL)—CRED, Brussels, Belgium, www.emdat.be.
[2] United States, *Federal Emergency Management Agency FEMA*. www.fema.gov.
[3] S. Bird; E. Klein; E. Loper, *Natural Language Processing with Python*. O'Reilly Media Inc., www.nltk.org/book.
[4] K. Homann; A. Lulay, *Understanding and Solving Algebra Story Problems by Neural Networks and Computer Algebra Systems*. Karlsruhe, Germany (1996).
[5] C. Chase.; S. Christley; G. An, *Facilitating automated conversion of scientific knowledge into scientific simulation models with the Machine Assisted Generation, Calibration, and Comparison (MAGCC) Framework*. arXiv: 2204.10382 (2022).

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul. Turkey | August 15–19, 2022
Session on *"Computer Algebra Applications in the Life Sciences"*

Nondegenerate Andronov–Hopf bifurcations in a class of bimolecular mass-action systems (Part I)

Murad Banaji[1]***, Balázs Boros***[2] [m.banaji@mdx.ac.uk]

[1] Department of Design Engineering and Mathematics, Middlesex University London
[2] Department of Mathematics, University of Vienna, Austria

We systematically address the question of which small, bimolecular, chemical reaction networks endowed with mass-action kinetics are capable of Hopf bifurcation. It is easily shown that any such network must have at least three species and at least four irreversible reactions. We are able to fully classify three-species, four-reaction, bimolecular networks: with the extensive help of computer algebra, we divide these networks into those which *forbid* Hopf bifurcation and those which *admit* Hopf bifurcation. We find that a previously known example due to Thomas Wilhelm is only one of many networks in this class which admit Hopf bifurcation.

The task of deciding which small networks admit Hopf bifurcation naturally breaks into two parts. First, we focus on ruling out Hopf bifurcation in the great majority of the networks; and second, we focus on confirming, where possible, that a nondegenerate bifurcation occurs in the remaining networks.

Part I. Beginning with 14,670 three-species, four-reaction, bimolecular networks which admit positive equilibria, we show that the great majority of these are incapable of Hopf bifurcation. Often we can declare the absence of Hopf bifurcation in a given network by proving the positivity of an associated polynomial. This task can be approached using software, including semidefinite programming, to decompose the polynomials into sums of squares and positive terms. At the end of this process, we are left 138 networks with the potential for Hopf bifurcation. These fall into 87 distinct classes, up to a natural equivalence.

Part II. Having shown that there are 87 distinct classes of three-species, four-reaction, bimolecular chemical reaction networks with the potential for Hopf bifurcation, the next question is how many of these networks actually admit a nondegenerate Hopf bifurcation. Out of the 87 classes we find that 86 admit nondegenerate Hopf bifurcation. The remaining exceptional network robustly admits a degenerate Hopf bifurcation.

Amongst the 86 networks capable of nondegenerate Hopf bifurcation, we find that 57 admit a supercritical Hopf bifurcation, 54 admit a subcritical Hopf bifurcation. At the intersection of these networks are 25 networks which admit both bifurcations and hence can have both stable and unstable periodic orbits. These claims involve extensive use of computer algebra to

automate the process of checking nondegeneracy and transversality conditions. With the help of these computations, we are able to show that many of the networks admit the coexistence of a stable equilibrium and a stable periodic orbit for some choices of rate constants. We also make some progress towards showing the occurrence of bifurcations of higher codimension in these networks.

Finally, we can use the results on three-species, four-reaction, bimolecular networks, along with previously developed theory, to predict the occurrence of Hopf bifurcation in networks with more species and/or reactions. Thus, in fact, finding all small networks with the capacity for Hopf bifurcation greatly expands our knowledge of which chemical reaction networks, not necessarily small, admit Hopf bifurcation.

Keywords
Hopf bifurcation, chemical reaction networks, oscillation

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul. Turkey | August 15–19, 2022
Session on *“Computer Algebra Applications in the Life Sciences”*

Nondegenerate Andronov–Hopf bifurcations in a class of bimolecular mass-action systems (Part II)

Murad Banaji[1]***, Balázs Boros***[2] [balazs.boros@univie.ac.at]

[1] Department of Design Engineering and Mathematics, Middlesex University London
[2] Department of Mathematics, University of Vienna, Austria

We systematically address the question of which small, bimolecular, chemical reaction networks endowed with mass-action kinetics are capable of Hopf bifurcation. It is easily shown that any such network must have at least three species and at least four irreversible reactions. We are able to fully classify three-species, four-reaction, bimolecular networks: with the extensive help of computer algebra, we divide these networks into those which *forbid* Hopf bifurcation and those which *admit* Hopf bifurcation. We find that a previously known example due to Thomas Wilhelm is only one of many networks in this class which admit Hopf bifurcation.

The task of deciding which small networks admit Hopf bifurcation naturally breaks into two parts. First, we focus on ruling out Hopf bifurcation in the great majority of the networks; and second, we focus on confirming, where possible, that a nondegenerate bifurcation occurs in the remaining networks.

Part I. Beginning with 14,670 three-species, four-reaction, bimolecular networks which admit positive equilibria, we show that the great majority of these are incapable of Hopf bifurcation. Often we can declare the absence of Hopf bifurcation in a given network by proving the positivity of an associated polynomial. This task can be approached using software, including semidefinite programming, to decompose the polynomials into sums of squares and positive terms. At the end of this process, we are left 138 networks with the potential for Hopf bifurcation. These fall into 87 distinct classes, up to a natural equivalence.

Part II. Having shown that there are 87 distinct classes of three-species, four-reaction, bimolecular chemical reaction networks with the potential for Hopf bifurcation, the next question is how many of these networks actually admit a nondegenerate Hopf bifurcation. Out of the 87 classes we find that 86 admit nondegenerate Hopf bifurcation. The remaining exceptional network robustly admits a degenerate Hopf bifurcation.

Amongst the 86 networks capable of nondegenerate Hopf bifurcation, we find that 57 admit a supercritical Hopf bifurcation, 54 admit a subcritical Hopf bifurcation. At the intersection of these networks are 25 networks which admit both bifurcations and hence can have both stable and unstable periodic orbits. These claims involve extensive use of computer algebra to

automate the process of checking nondegeneracy and transversality conditions. With the help of these computations, we are able to show that many of the networks admit the coexistence of a stable equilibrium and a stable periodic orbit for some choices of rate constants. We also make some progress towards showing the occurrence of bifurcations of higher codimension in these networks.

Finally, we can use the results on three-species, four-reaction, bimolecular networks, along with previously developed theory, to predict the occurrence of Hopf bifurcation in networks with more species and/or reactions. Thus, in fact, finding all small networks with the capacity for Hopf bifurcation greatly expands our knowledge of which chemical reaction networks, not necessarily small, admit Hopf bifurcation.

Keywords
Hopf bifurcation, chemical reaction networks, oscillation

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey | August 15-19, 2022
Session on *"Computer Algebra Applications in the Life Sciences"*

Polynomial Systems Theories in Biology

James H. Davenport[1] [J.H.Davenport@bath.ac.uk]

[1] Department of Computer Science, University of Bath, U.K.

Biochemical systems consist, from our point of view, of various substances in various concentrations. The concentrations satisfy systems of ordinary differential equations, which themselves depend on parameters. The qualitative behaviour of these systems is of great interest to the biologists, in particular whether they permit multiple (locally) steasy states.

How might computer algebra help understand these questions, both in theory and in practice? This talk will look at some answers to these questions, and pose more questions.

Keywords
systems biology, parameter space, multistationarity, computer algebra.

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2021
Session on *"Computer Algebra Applications in the Life Sciences"*

Open problems in parameteric dynamical systems from life sciences

Alexey Ovchinnikov[1] [aovchinnikov@qc.cuny.edu]

[1] CUNY Queens College, Department of Mathematics, Queens, NY 11367 and CUNY Graduate Center, Ph.D. Programs in Mathematics and Computer Science, 365 Fifth Avenue, New York, NY 10016, USA

The parameter identifiability problem of a dynamical system is to determine whether the parameters of the system can be found from a given subset of variables of the system. Differential algebra and symbolic computation have played a central role in tackling this problem. However, there are still many open questions that are important in the applications to life sciences. These questions pose challenges both in theory and implementation. We will highlight several of these questions.

Keywords
parameter identifiability, mathematical biology, differential algebra, difference algebra, symbolic computation

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey | August 15-19, 2022
Session on *"Computer Algebra Applications in the Life Sciences"*

Algebraic sequence modelling for disaster management

Klaus Kieseberg[1]***, Bernhard Garn***[1]***, Dimitris E. Simos***[1]
`[{kkieseberg,bgarn,dsimos}@sba-research.org]`

[1] SBA Research, Vienna, Austria

Training exercises are key instruments in crisis management as they assist in a multitude of tasks, such as planning pre-crisis resource requirements and allocation, response planning and helping train emergency personnel for actual crises [1]. To be effective, exercises must provide a safe but realistic environment and allow for conclusive evaluation. To this end, exercises have to utilize well constructed scenarios which are not only able to replicate certain characteristics of a crisis situation, but are also easily adaptable and provide ample training diversity [2]. Here, certain mathematical structures [3] derived from the field of combinatorial testing [4,5] can greatly help with the generation of such scenarios, since their abstract properties can be linked to certain characteristics of exercises and exercise scenarios.

In this talk, we will take a look at suitable combinatorial sequence structures and their usage in the domain of disaster management. We will present how computer algebra techniques can be used for the modelling and generation of these combinatorial sequence structures, which will then be translated into exercise scenarios. In particular, we will highlight how real-world requirements from the domain of disaster exercises are translated into semantically equivalent algebraic expressions. Finally, we will showcase the importance of the notion of (sequential) coverage in disaster relief strategies with an example based on a real-life disaster scenario of a bushfire.

Keywords
Disaster Management, Combinatorial Testing.

References

[1] DEPARTMENT OF HOMELAND SECURITY, *Homeland Security Exercise and Evaluation Program (HSEEP)*. Online; accessed 6-June-2021.
[2] EUROPEAN CENTRE FOR DISEASE PREVENTION AND CONTROL, *Handbook on simulation exercises in EU public health settings – How to develop simulation exercises within the framework of public health response to communicable diseases*. (2014) Online; accessed 10-June-2021.
[3] C. COLBOURNE; J. DINIZ, *Handbook of combinatorial designs*, 2nd Edition, Chapman and Hall/CRC, New York, (2006).

[4] D. R. KUHN; J. M. HIGDON; J. F. LAWRENCE; R. N. KACKER; Y. LEI, *Combinatorial Methods for Event Sequence Testing*, IEEE Fifth International Conference on Software Testing, Verification and Validation, pp. 601–609 (2012).
[5] F. DUAN; Y. LEI; R. N. KACHER; D. R. KUHN, *An Approach to T-Way Test Sequence Generation With Constraints*. IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW), pp. 241–250 (2019).

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2021
Session on *"Session Title"*

Algebraic Network Analysis for Anti-Money Laundering

Ceren Culha[1]***, Bernhard Garn***[1]***, Dimitris E. Simos***[1]

[1] SBA Research, Vienna, Austria, {mculha,bgarn,dsimos}@sba-research.org

Network models manifest in various areas within computer science, from the hardware level up to the application layer. Prominent examples for networks include social networks and – more recently – network structures derived from blockchain data. Especially in the case of cryptocurrencies, the relationships between buyers and sellers, as well as the underlying 'money flow', have come under scrutiny as of late, since cryptocurrencies can be misused for various criminal activities. One major interest there is the identification and prevention of money laundering activities involving cryptocurrencies, which currently poses severe challenges to anti money-laundering (AML) efforts. To this end, various graph based models and their properties have been proposed in the literature [6][7][8][9][10].

In this talk, we are interested in exploring algebraic versions of network or graph properties [3,5], that are of potential interest to AML efforts. In particular, we consider algebraic approaches for analyzing social network from the literature [11][1][2], for example the *Cayley color graph* for graphically representing the relationship structure in a network. We provide a survey-style overview of methods that have been used, together with some of the experienced challenges. Furthermore, in our analysis, we pay particular attention to generalizations of the considered properties to hypergraphs and multiplex-networks, since these structures provide additional modelling capabilities. We conclude with an outlook on possible future research directions.

Keywords
networks, graphs, anti money laundering, computer algebra, multiplex networks

References

[1] RIVERO OSTOIC, J. A, *Algebraic Analysis of Social Networks: Models, Methods and Applications Using R*. February 2021.
[2] RIVERO OSTOIC, J. A, Algebraic Analysis of Multiple Social Networks with Multiplex, *Journal of Statistical Software* **92**(11), 1–41.(February 2020).
[3] GODSIL CHRIS, ROYLE GORDON, Algebraic Graph Theory, 2001.
[4] ŞTEFĂNESCU GHEORGHE, Network Algebra, Springer London, 2000. https://doi.org/10.1007/978-1-4471-0479-7

[5] BIGGS, N, Algebraic Graph Theory (2nd ed., Cambridge Mathematical Library).Cambridge: Cambridge University Press. https://doi:10.1017/CBO9780511608704.

[6] WAGNER, D., (2019). Latent representations of transaction network graphs in continuous vector spaces as features for money laundering detection. In: Becker, M. (Hrsg.), SKILL 2019 - Studierendenkonferenz Informatik. Bonn: Gesellschaft für Informatik e.V.. (S. 143-154).

[7] LI, X., LIU, S., LI, Z., HAN, X., SHI, C., HOOI, B., HUANG, H., CHENG, X. (2020). FlowScope: Spotting Money Laundering Based on Graphs. Proceedings of the AAAI Conference on Artificial Intelligence, 34(04), 4731-4738. https://doi.org/10.1609/aaai.v34i04.5906

[8] WEBER, MARK DOMENICONI, GIACOMO CHEN, JIE WEIDELE, DANIEL BELLEI, CLAUDIO ROBINSON, TOM LEISERSON, CHARLES. (2019). Anti-Money Laundering in Bitcoin: Experimenting with Graph Convolutional Networks for Financial Forensics.

[9] WEBER, MARK CHEN, JIE SUZUMURA, TOYOTARO PAREJA, ALDO MA, TENGFEI KANEZASHI, HIROKI KALER, TIM LEISERSON, CHARLES SCHARDL, TAO. (2018). Scalable Graph Learning for Anti-Money Laundering: A First Look.

[10] ALARAB, ISMAIL PRAKOONWIT, SIMANT. (2022). Graph-Based LSTM for Anti-money Laundering: Experimenting Temporal Graph Convolutional Network with Bitcoin Data. Neural Processing Letters. 1-19. 10.1007/s11063-022-10904-8.

[11] CASANELLAS, MARTA AND PETROVIĆ, SONJA AND UHLER, CAROLINE., Algebraic Statistics in Practice: Applications to Networks (March 2020). Annual Review of Statistics and Its Application, Vol. 7, Issue 1, pp. 227-250, 2020, Available at SSRN: http://dx.doi.org/10.1146/annurev-statistics-031017-100053

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *“Algorithms in Cryptography and Blockchain”*

A General Version of Carlet’s Construction of APN Functions

İlksen Acunalp Erleblebici[1]***, Oğuz Yayla***[1] [ilksenerleblebici@gmail.com]

[1] Cryptography Department, Middle East Techinical University, Ankara, Türkiye

APN functions have an important place in the fields of coding theory, cryptography,sequence design, combinatorics, algebra and projective geometry. Carlet [1] proposed a construction of APN functions using the bent functions $B(x, y) = xy$. With Theorem 5.6 in [4], they considered the general bivariate construction from [1],and they revealed its relation to the infinite families of bivariate APN functions in [2] and [3]. We propose a more general version of Carlet’s construction.

Theorem 1. *Let* $F(x, y) = (xy, a(x^{2^i+1})^{2^k}) + b(x^{2^i}y)^{2^h} + c(xy^{2^i})^{2^r} + d(y^{2^i+1})^{2^s})$ *be an APN function over* $F_{2^{2m}}$*. Then,* F *is EA-equivalent to one of the following functions*

$F_1(x, y) = (xy, x^{2^i+1} + x^{2^{i+h}}y^{2^h} + b'x^{2^k}y^{2^{i+k}} + c'y^{2^{i+r}+2^r})$,
$F_2(x, y) = (xy, x^{2^i+1} + x^{2^k}y^{2^{i+k}} + c'y^{2^{i+r}+2^r})$
$F_2(x, y) = (xy, x^{2^i+1} + c'y^{2^{i+r}+2^r})$ *with* $c' \neq 0$.

In [4] it is given a necessary condition for a function F_1 with $h = m/2$, $k = 0$, $r = 0$ to be APN. They checked the conditions 1,2,3 of Section 1 in [1]. The condition 1 and 2 are clearly satisfied. We dealth with the third condition.
$F_1(x, y) = (xy, x^{2^i+1} + x^{2^{i+h}}y^{2^h} + b'x^{2^k}y^{2^{i+k}} + c'y^{2^{i+r}+2^r})$
$G(x, y) = x^{2^i+1} + x^{2^{i+h}}y^{2^h} + b'x^{2^k}y^{2^{i+k}} + c'y^{2^{i+r}+2^r}$
$G(x, \beta x) = x^{2^i+1} + \beta^{2^h}x^{2^{i+h}}x^{2^h} + b'\beta^{2^{i+k}}x^{2^k}x^{2^{i+k}} + c'\beta^{2^{i+r}+2^r}x^{2^{i+r}+2^r}$
$G(x, \beta x) = L_\beta(x^{2^i+1})$, we take $x^{2^i+1} = x$
$L_\beta(x) = x + \beta^{2^h}x^{2^h} + b'\beta^{2^{i+k}}x^{2^k} + c'\beta^{2^{i+r}+2^r}x^{2^r}$.
We found out that the condition is satisfied when $h/k/r/m$ or $h = k = r/m$.
Actually F_1 is APN if and only if L_β is a permutation of F_{2^m}. L_β is a linearized polynomial.
We extended the Theorem 6.2 in [4] with $h = m/4$, $k = 2m/4$, $r = 3m/4$.
$L_\beta(x) = x + Ax^{2^{m/4}} + Bx^{2^{2m/4}} + Cx^{2^{3m/4}}$ and A, B, C are coefficients depending on b', c', β. L_β is a permutation if and only if

$$\begin{vmatrix} 1 & A & B & C \\ C^{2^{m/4}} & 1 & A^{2^{m/4}} & B^{2^{m/4}} \\ B^{2^{m/2}} & C^{2^{m/2}} & 1 & A^{2^{m/2}} \\ A^{2^{3m/4}} & B^{2^{3m/4}} & C^{2^{3m/4}} & 1 \end{vmatrix}$$

is nonzero.

Keywords
APN Functions, Permutation polynomial, Linearized polynomial

References

[1] C. CARLET, Relating three nonlinearity parameters of vectorial functions and building APN functions from bent functions. *Des. Codes Cryptogr.* (59), 89–109 (2011).
[2] Y. ZHOU, A. POTT, A new family of semifields with 2 parameters. *Adv. Math.* (234), 43–60 (2013).
[3] H. TANIGUCHI, On some quadratic APN functions *Des. Codes Cryptogr.* (87), 1973–1983 (2019).
[4] M. CALDERINI, L. BUDAGHYAN, AND C. CARLET, On known constructions of APN and AB functions and their relation to each other. *IACR Cryptol. ePrint Arch. 2020: 1444 (2020)*

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2021
Session on *“Session Title”*

Handover Authentication Protocols in Mobile Networks

Hakan Yıldırım[1], ***Murat Cenk***[1] [hakan.yildirim@metu.edu.tr]

[1] Institute of Applied Mathematics, Middle East Technical University, Ankara, Turkey

With the announcement of new generations in mobile wireless networks, new capabilities, higher bandwidth capacity, and increased robustness are expected [1]. In order to reach those ambitions, a huge number of small base stations which work in high frequencies and low coverage areas are used [2]. Mobile device users need to encounter more frequent handovers. The increase in the frequency of handovers and expectations from the new mobile wireless networks necessitates possessing a handover protocol that is secure, and efficient. In order to create such a handover protocol, it is required to understand the cryptographic methods used in handover authentication protocols, performance, and security requirements of a handover protocol. In this work, our aim is to give useful information regarding handover authentication, security, and performance characteristics of handover authentication methods, and cryptographic algorithms used in handover authentication. We study handover authentication protocols based on bilinear pairing cryptography. We analyze protocols satisfying all security requirements of a secure handover authentication protocol which are Mutual Authentication, User Anonymity, Non Traceability, Conditional Privacy Presentation, Session Key Establishment, Perfect Forward Secrecy, and Attack Resistance [3]. We also discuss possible optimizations of this approach and show that network consumption and computation complexity can be further diminished.

Keywords
Handover Authentication Protocols, Mobile Networks, Bilinear Pairing

References

[1] SATHIYA, M., ET AL., Cellular and network architecture for 5G wireless communication networks in mobile technology. *International Journal of Technical Research and Applications* **volume**(3.2), 206-11 (2015).
[2] FAN, CHUN-I., ET AL., ReHand: Secure Region-based Fast Handover with User Anonymity for Small Cell Networks in 5G *IEEE Transactions on Information Forensics and Security* **volume**(15), 927-942 (2019).
[3] HE, DEBIAO, ET AL., Anonymous handover authentication protocol for mobile wireless networks with conditional privacy preservation. *Science China Information Sciences* **volume**(60.5), 1-17 (2017).

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2021
Session on *"Algorithms in Cryptography and Blockchain"*

A Three-Party Lattice-Based Hybrid PAKE Protocol with Anonymity

Kübra Seyhan[1]***, Sedat Akleylek***[1] [kubra.seyhan@bil.omu.edu.tr]

[1]Department of Computer Engineering, Ondokuz Mayıs University, 55139, Samsun, Turkey

Key exchange (KE) protocols are one of the basic principles of public-key cryptography used to achieve secure communication by providing parties with a shared key. Authenticated key exchange (AKE) and password-based AKE (PAKE) versions are constructed to ensure that the parties and the adversary are not part of the communication [1]. PAKE protocols are not commonly used because there is no usable and suitable version of widespread applications. Those are generally preferred in some areas, such as e-passport applications, web browser synchronization, and Wi-Fi communication [3]. The first PAKE protocol is proposed as a traditional Diffie-Hellman KE version by relying on the hardness of the discrete logarithm problem (DLP). In that protocol, a password with low entropy and easy memorability was used to get authentication [2]. With the proposal of Shor algorithm in 1994, it was realized that the DLP problem will be solved in the presence of large quantum computers. As a result of this development, researchers and companies started to make provisions to maintain the security of public key cryptographic (PKC) primitives in the post-quantum era. The main method to construct post-quantum secure protocols is obtained by changing the computational hard mathematical problem with some problems which do not solve by using quantum computing power. Lattice, code, hash, and multivariate-based hard problems are generally used to propose new post-quantum secure PKC protocols. Thanks to strong security guarantees and worst-case hardness properties of the lattice-based cryptosystem family, they are commonly preferred in constructing post-quantum secure protocols [4].

The main advantages of lattice-based PAKE protocols against AKE are low communication cost and storage space, which are obtained thanks to low entropy passwords. Different lattice-based KE protocols were initially proposed to obtain solutions against post-quantum secure KE requirements. Adding structures such as hash functions and digital signatures, AKE and PAKE versions of these approaches, which can be used for two or multiple parties' communication, were constructed to procure authentication. In [5], a lattice-based two-party PAKE protocol with the anonymity property was proposed. The hardness assumption of this protocol is based on the ring version of the learning with errors (RLWE) problem. In that protocol, the practical randomized KE design approach was used to add resistance against mobile users' signal leakage attack (SLA). To overcome reconciliation problem, Sig and Mod$_2$ functions were used. According to the presented security analysis, the proposed protocol can be used to obtain post-quantum secure mobile network communication. However, in real-world

applications, the number of devices in the network is much more than two parties. The first step to overcome this problem is to create protocol designs in which the number of communicating parties increases. In [6], a three-party lattice-based PAKE protocol was constructed. It is also based on RLWE hardness and uses Cha and Mod_2 functions to obtain agreement between the parties. In the proposed protocol, the server allows two different mobile users to receive the shared key using timestamps. The design methodology of [6] is also an appropriate and recently used method to secure two mobile users and one server communication. The main aim of this paper, by combining approaches [5] and [6], is to obtain a three-party PAKE protocol with the anonymity feature.

In this paper, a hybrid lattice-based three-party PAKE protocol is proposed to provide the KE requirement of mobile devices in the post-quantum era. We choose [5] and [6] PAKE protocols to construct hybrid protocol. The main aim is to design a scheme that generates the shared key between two mobile users thanks to the server's guidance using low entropy passwords. By using [6] design approach, we increase the number of communicated parties of [5]. The hardness assumption of the proposed PAKE is based on the RLWE problem. It uses Sig and Mod_2 reconciliation structures to obtain the shared key. Unlike [6], the proposed hybrid protocol has anonymity due to the additional identity component of [5]. Thanks to the randomized KE components, an adversary does not make any SLA attack against the proposed PAKE.

Keywords
post-quantum cryptography, lattice-based cryptography, password authenticated key exchange, ring learning with errors, anonymity

Acknowledgements
This work was partially supported by TÜBİTAK under grant no. 121r006

References

[1] Abdalla, M., Pointcheval, D. (2005, February). Simple password-based encrypted key exchange protocols. In Cryptographers' track at the RSA conference (pp. 191-208). Springer, Berlin, Heidelberg.

[2] S. M. Bellovin and M. Merritt, "Encrypted key exchange: password-based protocols secure against dictionary attacks," Proceedings 1992 IEEE Computer Society Symposium on Research in Security and Privacy, 1992, pp. 72-84, doi: 10.1109/RISP.1992.213269.

[3] Hao, F., van Oorschot, P. C. (2021). SoK: Password-Authenticated Key Exchange–Theory, Practice, Standardization and Real-World Lessons. Cryptology ePrint Archive.

[4] Peikert, C. (2016). A decade of lattice cryptography. Foundations and Trends® in Theoretical Computer Science, 10(4), 283-424.

[5] Ding, R., Cheng, C., Qin, Y. (2022). Further Analysis and Improvements of a Lattice-Based Anonymous PAKE Scheme. IEEE Systems Journal. In Press.

[6] Islam, S. H., Basu, S. (2021). PB-3PAKA: Password-based three-party authenticated key agreement protocol for mobile devices in post-quantum environments. Journal of Information Security and Applications, 63, 103026.

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2021
Session on *"Algorithms in Cryptography and Blockchain"*

A Lattice-based Group Signature Scheme with Applications in Blockchain

Meryem Soysaldı Şahin[1]***, Sedat Akleylek***[1] [meryem.soysaldi@bil.omu.edu.tr]

[1] Department of Computer Engineering, Ondokuz Mayis University, Samsun, Türkiye

Digital signatures are used to ensure the integrity of the message, non-repudiation of the sender, and verify the sender's identity. Most existing digital signature schemes are based on hard problems such as discrete logarithm and factorization problems. With the increasing development of internet technologies, the need for digital signatures is increasing daily. Many digital signature schemes, such as group, ring, blind, proxy, and multi-signature, are proposed for different purposes in the literature.

The concept of group signature was introduced by Chaum and van Heyst [1]. With the group signatures, any group member can sign messages on behalf of the group. Group members are guaranteed to be a member of a specified group without revealing their identity. Moreover, the group manager reveals the identities of the group members who sign the message in case of a dispute. The group signatures must satisfy anonymity, traceability, and non-frameability [2]. Due to its advantages, group signatures are used in many real-life applications such as anonymous online communication, trusted computing platforms, privacy protection mechanisms, digital rights management, and auction protocols (voting, bidding, and anonymous approval) [3]. Group signatures can be used in blockchain, having specific applications in finance and e-commerce. Since most of the identification schemes used in the blockchain are based on public key-based signatures, it primarily aims to reveal the transaction identity. However, the signer's public key remains anonymous as the group signatures can only verify the signer's group. In this study, we propose a lattice-based group signature scheme that can be used in blockchain. The hardness of the proposed scheme depends on the SIS and LWE problems. Besides, we prove security of the proposed scheme in random oracle model. With the proposed group signature scheme, we ensure the privacy of requesters who are not performed in many blockchain markets. In other words, bidders can only access group information instead of requester's identities.

Keywords
group signature, blockchain, lattice-based cryptography, anonymity, traceability, non-frameability

Acknowledgments
This study was partially supported under grant no.121R006 by TUBITAK.

References

[1] D. Chaum; E. V. Heyst, Group signatures. *Advances in Cryptology — EUROCRYPT '91. Lecture Notes in Computer Science*. **volume**(547), 257–265 (1991).

[2] D. Boneh; X. Boyen; H. Shacham, Short group signatures. *In M. Franklin, editor, Proceedings of Crypto 2004. Lecture Notes in Computer Science* **volume**(3152), 41–55 (2004).

[3] M. N. S. Perera; T. Nakamura; M. Hashimoto; H. Yokoyama; C. M. Cheng; K. Sakurai, A Survey on Group Signatures and Ring Signatures: Traceability vs. Anonymity. *Cryptography* **volume**(6), 1–22 (2022).

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2022
Session on *“Algorithms in Cryptography and Blockchain”*

Two Post-Quantum Code-Based Cryptosystems

Sedat Akleylek[1]***, Ebubekir Aydoğmuş***[2]***, Ahmet Sınak***[2] [akleylek,aydogmus,sinakahmet@gmail.com]

[1] Department of Computer Engineering, Ondokuz Mayıs University, Samsun, Turkey
[2] Department of Mathematics and Computer Science, Necmettin Erbakan University, Konya, Turkey

The classical public key cryptosystems such as RSA and DSA are based on computationally hard problems such as integer factorization problem and discrete logarithm problem. These hard problems can be broken in polynomial time on quantum computers. To introduce quantum-secure public key cryptosystems, some quantum-safe hard problems have been used in the literature. One of them is syndrome decoding problem. Code-based cryptography was introduced in 1978 by McEliece [1] using binary Goppa codes. The security of the McEliece cryptosystem [1] relies on the hardness of decoding a random linear code. Code-based systems are of great importance in terms of working principle and providing efficient results, so efficient code families have been used when developing a new cryptosystem. Further code-based quantum-secure cryptosystems such as Niederreiter [2], Mcnie [3], RQC, HQC have been proposed. McEliece and Niederreiter cryptosystems are two famous quantum-safe cryptosystems. They are robust and versatile cryptosystems. They work with any linear error-correcting codes.

McNie cryptosystem [3] was proposed as a new code-based public key encryption scheme. McNie is a hybrid version of the McEliece and Niederreiter cryptosystems and its security is reduced to the hard problem of syndrome decoding. The 3-semi-cyclic and 4-semi-cyclic LPRC codes were used in the McNie cryptosystem with a probabilistic decoding algorithm, which is a disadvantage for this system. A message recovery attack has been made to the McNie cryptosystem and it reduces the size of the random matrix. Due to this attack, it was proposed to redesign the McNie cryptosystem, and so the Mcnie-2 algorithm was proposed by using the Gabudilin code family instead of the LPRC code family.

In this work, we propose two new code-based public key encryption algorithms, called McNie variant-1 and McNie variant-2. The working principle of these systems is basically based on the McNie cryptosystem. The McNie system uses 3-semi-cyclic and 4-semi-cyclic classes of LPRC codes, a special class of the BCH code family. Unlike McNie, we use the Goppa code family in the proposed cryptosystems. In addition, to ensure the the desired security, the encryption phase is performed by dividing the message into two parts: identity and message.

Keywords

Post-quantum cryptography, Code-based cryptosystem, Quantum secure encryption, LPRC codes

Acknowledgements

This work is partially supported by TÜBİTAK under the grand number 121R006.

References

[1] R. J. McEliece, A public-key cryptosystem based on algebraic. *Coding Thv* **4244**, 114-116 (1978).
[2] H. Niederreiter, Knapsack-type cryptosystems and algebraic coding theory. *Prob. Contr. Inform. Theory* **15**(2), 157-166 (1986).
[3] L. Galvez; J. L. Kim; M. J. Kim; Y. Kim; N. Lee; R. Perlner, McNie: Compact McEliece-Niederreiter Cryptosystem. *NIST Post-Quantum Cryptography Project, First Round Candidate Algorithms.* (2017).

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2021
Session on *"General Session"*

A Call for more Automata Theory in Sequential Combinatorial Testing

Ludwig Kampel[1]***, Manuel Leithner***[1]***, Dimitris E. Simos***[1] [lkampel@sba-research.org]

[1] MATRIS, SBA Research, 1040 Vienna, Austria

Automata theory is well-established as a means to model and test software systems [1]. In the past, researchers have used automata to model a system under test (SUT), e.g. event-driven software systems such as internet protocols [1], [2]. In other works, automata have been used to describe the generation of test inputs for event-driven SUTs [3], [4]. Vice versa, we may even advance our understanding of automata theory via techniques used in software testing. For example, a work by Neeman uses ideas from equivalence partitioning to minimize (deterministic) finite automatons [5].

The terminology of automata theory lends itself to the description of software artifacts. For example, the grammar of a programming language is often specified in a notation such as the Backus-Naur form. Similarly, program behavior can be described using finite state machines (FSMs). However, many works apply automata theory merely to provide a problem description, foregoing the opportunity to utilize methods from this field to develop elegant solutions. In other cases, some results from this domain are successfully applied, but a more rigorous treatment holds the potential to increase the efficacy of devised methods.

For example, Yu et al. [3] use an automata theory formulation for their proposed approach for t-way test sequence generation utilized in sequential combinatorial testing. In this setting, one is interested in finding a minimized set of sequences over a finite alphabet such that all sequences of length t appear as a subsequence in at least one of the sequences in the test set [3], [4]. More formally, we can give a definition of *t-way sequence test sets* similar to that in the original work [3].

Definition. *Consider a (non-deterministic) finite automaton $\mathcal{A} = (Q, M, q_0, F)$, with a finite set of states Q, a transition matrix $M \in \mathscr{P}(\Sigma)^{Q\times Q}$ where Σ is the input alphabet, q_0 the initial state and F the set of final states. A* sequential t-way test set Π *is a set of words accepted by $\mathcal{A}$, such that for each t-sequence $\sigma \in \Sigma^t$ that can appear as a subsequence of an accepted word, there exists at least one such word in* Π.

We believe that the presented approach [3] has great merit and provides a useful framework for the construction of t-way test sequences. At the same time, we believe that by applying results from automata theory, some of the presented algorithms can be modified and sped-up. For example, the algorithm presented for target sequence generation in the original work [3] can be improved by taking the t-th power of the *transition matrix* describing the transitions of the given finite automaton.

Another work [4] presents an automata theory approach for generating t-way sequences for event-driven software testing. In order to generate a sequential t-way test set that is in accordance with the SUT's constraints, an automaton modeling the SUT is intersected with an automaton that accepts all words that contain a specific target t-sequence $\sigma \in \Sigma^t$ as a sub-word, called *t-sequence automaton* (respectively t-wise automaton in [4]). This process can be iterated with additional t-sequence automata. A test sequence is then obtained by selecting a (shortest) word accepted by the automaton resulting from these intersections. By construction, this test sequence is accepted by the automaton modeling the SUT and contains multiple $\sigma \in \Sigma^t$ as a sub-words. As automata are incrementally intersected, this soon becomes time-consuming and certainly represents the bottleneck of the presented methodology. This process immediately raises the question how we can construct the intersection of these t-sequence automata more efficiently. We believe that this approach might be leveraged even further.

While the original work [4] represents a very elegant application of automata theory for the objectives of sequential combinatiorial testing, it is directly linked to theoretically interesting aspects of automata theory. As the resulting automata are mainly used in order to obtain a word of minimum length (or, in a weakened version, of minimized length) that is accepted by the automaton, the application described above also bears the following problem inherent to automata theory: *Given two languages L_1 and L_2, what is the shortest word in the intersection $L_1 \cap L_2$ of these two languages?*

The construction of (minimal) intersections of automata seems to be a well-known yet difficult problem [7], with several contributions on that topic [8]. However, there appear to be only basic results regarding the problem of words of minimal length accepted by the intersection of automata [9]. In the work on t-way sequences [4], at least one of the automata appearing in the intersection is a t-sequence automaton (thus bearing a very specific structure). Accordingly, there may be more efficient ways to determine a $w \in L_1 \cap L_2$ of minimal length for this particular application.

Keywords
Automata Theory, Combinatorial Testing, Test Sequence Generation

References

[1] T. S. Chow, Testing software design modeled by finite-state machines. *IEEE Transactions on Software Engineering* **volume**(3),178–187 (1978).
[2] G. Fraser, F. Wotawa, P.E. Ammann, Testing with model checkers: a survey. *Software Testing, Verification and Reliability,* **volume**(19(3)), 215–261 (2009).
[3] L. Yu, Y. Lei, R.N. Kacker, D.R. Kuhn, J. Lawrence, Efficient algorithms for t-way test sequence generation. In *2012 IEEE 17th International Conference on Engineering of Complex Computer Systems* 220–229 . IEEE. (2012).
[4] A. Bombarda, A. Gargantini, Title. In *2020 IEEE international conference on software testing, verification and validation workshops (ICSTW)*, 157–166. IEEE. (2020).
[5] A. Neeman, Buy one get one free: automata theory concepts through software test.

Journal of Computing Sciences in Colleges **volume**(31(6)), 90–96 (2016).

[6] J ALMAN, V. V. WILLIAMS, A refined laser method and faster matrix multiplication. In *Proceedings of the 2021 ACM-SIAM Symposium on Discrete Algorithms (SODA)*, Society for Industrial and Applied Mathematics. 522–539 (2021).

[7] R. J. LIPTON, On the intersection of finite automata. In *The P= NP Question and Gödel's Lost Letter*, Chapter 31, 145–148. Springer, Boston, MA. (2010).

[8] M. WEHAR, Hardness results for intersection non-emptiness. In *International Colloquium on Automata, Languages, and Programming* 354–362 . Springer, Berlin, Heidelberg. (2014).

[9] T. ANG, J. SHALLIT, Length of the shortest word in the intersection of regular languages. *arXiv preprint* arXiv:0910.1528 (2009).

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2021
Session on *"Session Title"*

Computer Algebra, Student Assessment and Learning Data Analysis

***David Smith*[1], *Stephen M. Watt*[2]** [smwatt@uwaterloo.ca]

[1] Digital Education Company Ltd, Cambridge, UK
[2] David R. Cheriton School of Computer Science, University of Waterloo, Canada

Online teaching and assessment tools are typically lacking for mathematical subjects in two different ways: The first is in producing sufficiently numerous questions of equivalent difficulty for a given topic. The second is to be able to evaluate student-generated answers that may have many mathematically equivalent forms. A computer algebra system is needed to do both these things well. The Möbius platform uses an embedded Maple system for this purpose. Möbius has been deployed to more than 400 educational institutions and has evaluated more than 35,000,000 student problems. This has been used to collect anonymized data for analysis. This data can be used to measure and identify factors in learner engagement and course pathways. We summarize one study of how this has been used to measure the relationship between uniformity of engagement and student outcomes [2]. The talk concludes with some forward-looking ideas on learner modelling.

Conflict of Interest Statement
The authors are related to Digital Education Company, Ltd, the Möbius service provider .

Keywords
online education, mathematics, teaching and assessment

References

[1] MÖBIUS, `https://www.digitaled.com/mobius` (retrieved 2022-08-04)
[2] DAVID SMITH, ARON PASIEKA, RALF BECKER, CHRISTINA PERDIKOULIAS, Student Success in Asynchronous STEM Education: measuring and identifying contributors to learner. In *2022 IEEE Global Engineering Education Conference (EDUCON)*, 473-479.

Applications of Computer Algebra – ACA 2022
Gebze-Istanbul, Turkey, | August 15-19, 2021
Session on *"General Session"*

Certified Hermite Matrices from Approximate Roots

Tülay Ayyıldız Akoğlu[1]***, Agnes Szanto***[2] [tulayaa@ktu.edu.tr]

[1] Department of Mathematics, Karadeniz Technical University, Trabzon, Turkey
[2] North Carolina State University, Raleigh, NC, USA

Let $\mathcal{I} = \langle f_1, \ldots, f_m \rangle \subset \mathbb{Q}[x_1, \ldots, x_n]$ be a zero dimensional radical ideal defined by polynomials given with exact rational coefficients. Assume that we are given approximations $\{z_1, \ldots, z_k\} \subset \mathbb{C}^n$ for the common roots $\{\xi_1, \ldots, \xi_k\} = V(\mathcal{I}) \subseteq \mathbb{C}^n$. In this paper we show how to construct and certify the rational entries of Hermite matrices for $\mathcal{I}$ from the approximate roots $\{z_1, \ldots, z_k\}$. When $\mathcal{I}$ is non-radical, we give methods to construct and certify Hermite matrices for $\sqrt{\mathcal{I}}$ from the approximate roots. Furthermore, we use signatures of these Hermite matrices to give rational certificates of non-negativity of a given polynomial over a (possibly positive dimensional) real variety, as well as certificates that there is a real root within an ε distance from a given point $z \in \mathbb{Q}^n$.

Keywords
Symbolic–Numeric Computation, Polynomial Systems, Approximate Roots, Hermite Matrices, Certification

List of Participants

Michela Ceria, *Politecnico di Bari*
Halime Ömrüuzun Seyrek, *Sabancı University*
Nicola Vassena, *Free University Berlin*
Ferdinando Zullo, *Università degli Studi della Campania "Luigi Vanvitelli"*
Miklos Bona, *University of Florida*
Daniel Panario , *Carleton University*
Teo Mora, *Università di Genova*
Máté László Telek, *University of Copenhagen*
Alexander Levin, *The Catholic University of America*
Lucia Moura, *University of Ottawa*
Oskar Henriksson, *University of Copenhagen*
Relinde Jurrius, *Netherlands Defence Academy*
Xiaohang Chen, *Dalhousie University*
Luis M. Pardo, *University of Cantabria*
Mukhtar Minglibayev, *Al-Farabi Kazakh National University*
Bart De Bruyn, *Ghent University*
Yosuke Sato, *Tokyo University of Science*
Mohammad Zadeh Dabbagh, *Sabancı University*
Zohreh Aliabadi, *Sabancı University*
Rhys Evans, *Sobolev Institute of Mathematics*
Antonio Jiménez-Pastor, *LIX, CNRS, École Polytechnique*
Katsusuke Nabeshima, *Tokyo University of Science*
Alessandro Neri, *Max Planck Institute for Mathematics in the Sciences*
Malihe Aliasgari, *Kean University*
Daniel Lichtblau, *Wolfram Research*
Daniel Robertz, *RWTH Aachen University*
Henning Ulfarsson, *Reykjavik University*
Anurag Bishnoi, *TU Delft*
AmirHosein Sadeghimanesh, *Coventry University*
Tereso del Río, *Coventry University*
Vincent Vatter, *University of Florida*
John Sheekey, *University College Dublin*
Matthias Seiss, *University of Kassel*
Cem Güneri, *Sabancı University*
Jaime Gutierrez, *University of Cantabria*
Philipp Nuspl, *Johannes Kepler University Linz*
Pietro Mercuri, *Sapienza Università di Roma*
Thierry Combot, *Université de Bourgogne*
Carlos Arreche, *The University of Texas at Dallas*
Alexandre Goyer, *Inria*
Akira Terui, *University of Tsuku*ba
Alexander Prokopenya, *Warsaw University of Life Sciences* - *SGGW*
Nikolai Fadeev, *RISC*

Berina Celic, *MATRIS Research Group, SBA Research, Vienna, Austria*
Merve Ceren Culha, *MATRIS Research Group, SBA Research, Vienna, Austria*
Klaus Kieseberg, *MATRIS Research Group, SBA Research, Vienna, Austria*
Marcin Choiński, *Warsaw University of Life Sciences*
Raphaël Pagès, *Université de Bordeaux*
Kosaku Nagasaka, *Kobe University*
Yang Liu, *KAUST*
Eduardo Sáenz-de-Cabezón, *Universidad de La Rioja*
Michel Beaudin, *École de technologie supérieure*
Lixin Du, *Johannes Kepler University Linz*
Jiayue Qi, *University of Linz*
Sonia L. Rueda, *Universidad Politécnica de Madrid*
Elena Varbanova, *Technical University of Sofia*
Emre Yivli, *Eskişehir Technical University*
Victor Edneral, *Lomonosov Moscow State University*
Yasemin Büyükçolak, *Research assistant - Gebze Technical University*
Fatih Yetgin, *Research assistant - Gebze Technical University*
Büşra Şen, *Research assistant - Gebze Technical University*
Uğur Odabaşı, *İstanbul University-Cerrahpaşa*
Gianira Alfarano, *University of Zurich*
Manal Loukili, *Sidi Mohamed Ben Abdellah University*
Yağmur Sak, *Sabancı University*
Seyedeh Kosar, *University of Kashan*
Gülsemin Çonoğlu, *Sabancı University*

SPONSORS

PLATINUM

EUROPEAN MATHEMATICAL SOCIETY

INTERNATIONAL MATHEMATICAL UNION CDC

GOLD

TÜRK MATEMATİK DERNEĞİ

acm SIGSAM

SILVER

MATRIS

SBA Research

CARGO Lab
Computer Algebra Research Group

BRONZE

Maplesoft