The 28th International Conference on Applications of Computer Algebra ACA'2023

PROGRAM & ABSTRACTS

Warsaw University of Life Sciences – SGGW
Institute of Information Technology
July 17 – 21, 2023

WWW: https://aca2023.iit.sggw.pl

Program and Organizing Committees

General Chair

Alexander Prokopenya, Warsaw University of Life Sciences – SGGW, Poland

Scientific Committee: ACA Working group

Gabriel Aguilera Venegas
Alkiviadis Akritas
Michel Beaudin
Anouk Bergeron-Brlek
Francisco Botana
Bruno Buchberger
Thierry Dana-Picard
Victor Edneral
Jose Luis Galan Garcia
Victor Ganzha
Mark Giesbrecht
Hoon Hong
David Jeffrey
Erich Kaltofen
Ilias Kotsireas (co-chair)
Hiroshi Kai
Robert H. Lewis
Richard Liska
Edgar Martinez-Moro
Manfred Minimair
Aleksandr Myllari
Veronika Pillwein
Alexander Prokopenya
Louis-Xavier Proulx
Pedro Rodriguez Cielos
Tateaki Sasaki
Yosuke Sato
Werner Seiler
Tony Shaska
Dimitris Simos
Margarita Spiridonova
Stanly Steinberg
Quoc-Nam Tran
Elena Varbanova
Nikolay Vasiliev
Stephen Watt
Michael Wester (co-chair)
Wolfgang Windsteiger
Zafeirakis Zafeirakopoulos

Advisory Committee

Ilias Kotsireass, Waterloo, Canada
Michael Wester, New Mexico, USA

Local Organizing Committee

Ryszard Kozera (co-chair)
Alexander Prokopenya (co-chair)
Andrzej Zembrzuski
Marcin Ziółkowski
Artur Wiliński
Włodzimierz Wojas
Marcin Choiński
Monika Krawiec
Aleksandra Konopka
Karol Struniawski
Anna Dyniec
Monika Hertel-Świerad
Magdalena Magnuszewska
Robert Budzyński
Tomasz Minkowski

ACA2023 – General Schedule

Times	Monday	Tuesday	Wednesday	Thursday	Friday
09:00 – 09:30		S6, S9, S10	S4	S6, S10	
09:30 – 10:00	Registration, 3rd floor Aula IV Build. 34		S3, S8	S8, S3	S2
10:00 – 10:30					
10:30 – 11:00					
11:00 – 11:30		Coffee break (room 3/82)			
11:30 – 12:00		Plenary Lecture Jon McLoone	Plenary Lecture Werner M. Sieler	Plenary Lecture Adam Strzeboński	Closing
12:00 – 12:30	OPENNING Aula IV				
12:30 – 14:00	Lunch (Limba)				
14:00 – 14:30	S1, S7, S9	S6, S2, S10	S3, S8, S2	Excursion: Warsaw City Center, Royal Castle; Conference dinner at the Green GardenHotel Restaurant 19:00-22:30	
14:30 – 15:00					
15:00 – 15:30					
15:30 – 16:00	Coffee break (room 3/82)				
16:00 – 16:30	S1, S7, S9	S1, S9, S10	S10, S8, S2		
16:30 – 17:00					
17:00 – 17:30					
17:30 – 18:00					
18:00 – 19:00	Welcome reception (Limba)		ACA-WG meeting Aula IV		

S1 – Computer Algebra in Education
S2 – Computer Algebra Modeling in Science and Engineering
S3 – D-Finite Functions and Beyond: Algorithms, Combinatorics and Arithmetic
S4 – Computer Algebra Systems and Interval Methods
S6 – Computer Algebra Applications in the Life Sciences
S7 – Computational Differential and Difference Algebra and its Applications
S8 – Algebraic Geometry from an Algorithmic Point of View
S9 – Effective Ideal Theory and Combinatorial Techniques in Commutative and Non-Commutative Rings and Their Applications
S10 – Algebraic and Algorithmic Aspects of Differential and Integral Operators

Schedule for Invited Talks

Tuesday, July 18, 2023

Build. 34, 3d floor, Lecture Hall "Aula IV"

11:30 – 12:30 **Jon McLoone**
Wolfram's Vision for Unified Computation

Wednesday, July 19, 2023

Build. 34, 3d floor, Lecture Hall "Aula IV"

11:30 – 12:30 **Werner M. Seiler**
Theoretical and Numerical Analysis of Singular Initial and Boundary Value Problems

Thursday, July 20, 2023

Build. 34, 3d floor, Lecture Hall "Aula IV"

11:30 – 12:30 **Adam Strzebonski**
Recent Symbolic Computation Developments in Mathematica

Schedule for Computer Algebra in Education Session

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

Monday, July 17

Build. 34, 3d floor, Lecture Hall "Aula IV"

14:00 – 14:30	**Elena Varbanova**, Stoyan Kapralov, Stanislav Simeonov Assessment of students' knowledge and abilities in undergraduate mathematics
14:30 – 15:00	**Setsuo Takato**, Hideyo Makishita Online drills created by extended CindyJS and scoring them with Maxima
15:00 – 15:30	**Eli Bagno**, Thierry Dana-Picard, Shulamit Reches ChatGPT excels in medicine but falters in basic algebra
15:30 – 16:00	Coffee Break
16:00 – 16:30	Johannes Middeke, **David J. Jeffrey**, Aishat Olagunju Orthogonal matrices: third time around
16:30 – 17:30	**Michel Beaudin** Using CAS in the classroom: personal thoughts (Part III)
17:30 – 18:00	**Josef Böhm** Surfaces and their Duals

Tuesday, July 18

Build. 34, 3d floor, Lecture Hall "Aula III"

16:00 – 16:30	**David J. Jeffrey**, Albert D. Rich Rubi gems
16:30 – 17:00	**Thierry Dana-Picard**, Tomas Recio Automated computation of geometric Loci in Mathematics Education
17:00 – 17:30	Zoltán Kovács, Tomás Recio, **M. Pilar Vélez** GeoGebra Automated Reasoning Tools: why and how (to use them in the classroom)
17:30 – 18:00	**Magdalena Skrzypiec**, W. Mozgawa, A. Naiman, P. Pikuta Orthogonal trajectories to isoptics of ovals
18:00 – 18:30	**Hideyo Makishita** Using CAS in mathematics education with the quadratic curve addition method

Schedule for Computer Algebra Modeling in Science and Engineering Session

Organized by Alexander Prokopenya, Haiduke Sarafian

Tuesday, July 18

Build. 34, 3d floor, Room 3/40

14:00 – 14:30 **Ryszard Kozera**
Fitting sparse reduced data

14:30 – 15:00 **Marcin Choinski**
A discrete SIS model built on the strictly positive scheme

15:00 – 15:30 **Marcin Ziółkowski**
On applications of computer algebra systems in queueing theory calculations

Wednesday, July 19

Build. 34, 3d floor, Room 3/40

14:00 – 14:30 **Haiduke Sarafian**
Analyzing electric circuits with computer algebra

14:30 – 15:00 **Setsuo Takato**, Hideyo Makishita
LMS with simple modeling developed by extended CindyJS and Maxima

15:00 – 15:30 Setsuo Takato, **Jose A. Vallejo**
Billiards: At the intersection of Math, Physics and Computer Algebra

15:30 – 16:00 Coffee Break

16:00 – 16:30 Tatjana Petek, **Valery G. Romanovski**
Computation of normal forms for systems with many parameters

16:30 – 17:00 Alina Ivashkevich, Victor Red'kov, **Alexander Chichurin**
Spin 1 particle with anomalous magnetic moment in external uniform electric field: solutions with cylindric symmetry

17:00 – 17:30 **Alexander Prokopenya**
On stability of stationary motion of the 3D swinging Atwood machine

17:30 – 18:00 **AmirHosein Sadeghimanesh**, Matthew England
Semi-algebraic representations for the multistationarity region of reaction networks

Friday, July 21

Build. 34, 3d floor, Room 3/40

09:30 – 10:00 **Aigerim Ibraimova**, Alexander Prokopenya, Mukhtar Minglibayev
Derivation of the evolution equations in the restricted three-body problem with variable masses by using Computer Algebra

10:00 – 10:30 **Aiken Kosherbayeva**, Mukhtar Minglibayev, Alexander Prokopenya
The problem of many bodies with isotropically varying masses

10:30 – 11:00 **Zhanar Imanova**, Alexander Prokopenya, Mukhtar Minglibayev
Investigation of a two-planetary problem of three bodies with variable masses varying anisotropically at different rates

11:00 – 11:30 Coffee Break

Schedule for D-Finite Functions and Beyond: Algorithms, Combinatorics and Arithmetic Session

Organized by Shaoshi Chen, Frédéric Chyzak, Antonio Jiménez-Pastor, Manuel Kauers, Veronika Pillwein

Wednesday, July 19

Build. 34, 3d floor, Lecture Hall "Aula IV"

09:30 – 10:00 Shaoshi Chen, **Lixin Du**, Manuel Kauers
Reduction based creative telescoping for definite summation of P-recursive sequences: the integral basis approach (online)

10:00 – 10:30 **Armin Straub**
Automatic Lucas-type congruences

10:30 – 11:00 **Philipp Nuspl**
Linear recurrence sequences in the OEIS

Wednesday, July 19

Build. 34, 3d floor, Lecture Hall "Aula IV"

14:00 – 14:30 **Hadrien Brochet**, Bruno Salvy
Reduction based creative telescoping for definite summation of D-finite functions: the Lagrange identity approach

14:30 – 15:00 **Catherine St-Pierre**
How a linear recurrence problem inspired a solution in algebraic geometry

15:00 – 15:30 **Qing-Hu Hou**, Guo-Jie Li, Na Li, Ke Liu
Two applications of the telescoping method

Thursday, July 20

Build. 34, 3d floor, Room 3/40

09:30 – 10:00 **Florent Brehard**, Nicolas Brisebarre, Mioara Joldes
A symbolic-numeric validation algorithm for linear ODEs with Newton-Picard method

10:00 – 10:30 Clemens G. Raab, **Georg Regensburger**
Algebraic consequences of the fundamental theorem of calculus in differential rings

10:30 – 11:00 **Manfred Buchacher**
Separating variables in bivariate polynomial ideals: the local case

Schedule for Computer Algebra Systems and Interval Methods

Organized by Milan Hladik, Małgorzata Jankowska, Vladik Kreinovich, Bartłomiej Kubica, Nathalie Revol, Iwona Skalna

Wednesday, July 19

Build. 34, 3d floor, Room 3/40

09:00 – 09:30 **Małgorzata A. Jankowska**, Bartłomiej J. Kubica, Andrzej Marciniak, Tomasz Hoffmann
On the application of an interval finite difference method and symbolic methods for solving the heat conduction problem

09:30 – 10:00 **Tomasz Hoffmann**, Andrzej Marciniak, Małgorzata A. Jankowska
On the application of directed interval arithmetic for solving elliptic BVP

10:00 – 10:30 **Bartłomiej Jacek Kubica**
Symbolic and algorithmic differentiation for the interval algorithm of training contracting autoencoders

10:30 – 11:00 **Laurent Granvilliers**
Symbolic recipes for solving nonlinear systems of equations with interval methods (online)

Schedule for Computer Algebra Applications in the Life Sciences

Organized by AmirHosein Sadeghimanesh, Andrzej Mizera, Ali Kemal Uncu

Tuesday, July 18

Build. 34, 3d floor, Lecture Hall "Aula III"

09:00 – 09:30 **Ovidiu Radulescu**
Inferring stochastic models of gene transcription from initiation events by computer algebra

09:30 – 10:00 **Alexandru Iosif**
Duality in mass-action networks

10:00 – 10:30 Marta Casanellas, Roser Homs Pons, **Angélica Torres**
Phylogenetic invariants for time-reversible models

10:30 – 11:00 **Andrzej Mizera**
Divide and control: an efficient decomposition-based approach towards the control of asynchronous Boolean networks

Tuesday, July 18

Build. 34, 3d floor, Lecture Hall "Aula III"

14:00 – 14:30 **Adam L. MacLean**
Gene regulatory network inference with joint multi-omic single-cell data to learn dynamic cell state transitions

14:30 – 15:00 **Jiayue Qi**, Josef Schicho
Five equivalent representations of a phylogenetic tree

15:00 – 15:30 **Marcus Aichmayr**, Georg Regensburger
Computing sign vector conditions for existence and uniqueness of equilibria of chemical reaction networks

Thursday, July 20

Build. 34, 3d floor, Lecture Hall "Aula IV"

09:00 – 09:30 **Nicola Vassena**
How to find or exclude bifurcations in biochemical systems?

09:30 – 10:00 **Oskar Henriksson**
Generic dimension of varieties arising in reaction network theory and 3D genome reconstruction

10:00 – 10:30 **Valery G. Romanovski**
Hopf bifurcations in some biochemical models

10:30 – 11:00 **Adam Strzeboński**
CAD adjacency computation using validated numerics

Schedule for Computational Differential and Difference Algebra and its Applications Session

Organized by Alexander Levin, Alexey Ovchinnikov, Daniel Robertz

Monday, July 17

Build. 34, 3d floor, Room 3/40

14:00 – 14:30 **Vladimir V. Bavula**
Classifications of prime ideals and simple modules of the Weyl algebra A1 in prime characteristic (online)

14:30 – 15:00 **Rida Ait El Manssour**, Gleb Pogudin
Multiplicity of arc spaces of fat points

15:00 – 15:30 **Alexander Levin**
A New Type of Difference Gröbner bases and their applications

15:30 – 16:00 Coffee Break

16:00 – 16:30 **Antoine Etesse**
On the Schmidt–Kolchin conjecture (online)

16:30 – 17:00 **Matthias Seiß**, Daniel Robertz
Specializations of normal forms in differential Galois theory

17:00 – 17:30 **V. Ravi Srinivasan**, Partha Kumbhakar
A classification of first order differential equations

17:30 – 18:00 **Valery G. Romanovski**
Local integrability of polynomial vector fields

Schedule for Algebraic Geometry from an Algorithmic Point of View Session

Organized by Cristina Bertone, Francesca Cioffi

Wednesday, July 19

Build. 34, 3d floor, Lecture Hall "Aula III"

09:30 – 10:00 **Emanuela De Negri**, Enrico Sbarra
Jet schemes of Pfaffian ideals

10:00 – 10:30 **Dušan Dragutinovic**
Binary curves of genera four and five

10:30 – 11:00 **Ignacio García-Marco**, Irene Márquez-Corbella, Edgar Martínez-Moro, Yuriko Pitones
Free resolutions and generalized Hamming weights of binary linear codes

11:00 – 11:30 Coffee Break

Wednesday, July 19

Build. 34, 3d floor, Lecture Hall "Aula III"

14:00 – 14:30 Amir Hashemi, **Matthias Orth**, Werner M. Seiler
Infinite free resolutions induced by Pommaret-like bases over Clements–Lindström rings

14:30 – 15:00 **Michela Ceria**, Francesco Pavese
The m-ovoids of $W(5,2)$ and their generalizations

15:00 – 15:30 **Teo Mora**, Michela Ceria, Andrea Visconti
Degroebnerization for data modelling problems

15:30 – 16:00 Coffee Break

16:00 – 16:30 **Teo Mora**, Michela Ceria
Generalizing Möller algorithm: a flexibility issue

16:30 – 17:00 **Meirav Amram**
On classification of algebraic curves and surfaces, using algorithmic methods

17:00 – 17:30 **Alberto Calabri**
On the weighted proximity graph of the base locus of a plane Cremona map

17:30 – 18:00 **Ozhan Genc**
Irreducible supernatural bundles on Grassmannians

Thursday, July 20

Build. 34, 3d floor, Lecture Hall "Aula III"

09:30 – 10:00 Davide Bolognini, Antonio Macchia, Giancarlo Rinaldo, **Francesco Strazzanti**
An algorithmic approach to characterize Cohen-Macaulay binomial edge ideals of small graphs

10:00 – 10:30 Philippe Gimenez, **Mario González-Sánchez**
Sumsets and the Castelnuovo-Mumford regularity of projective monomial curves

10:30 – 11:00 Amir Hashemi, Mahshid Mirhashemi, **Werner M. Seiler**
Applying machine learning to the computation of Pommaret bases – A progress report

Schedule for Effective Ideal Theory and Combinatorial Techniques in Commutative and Non-Commutative Rings and Their Applications Session

Organized by Michela Ceria, André Leroy, Samuel Lundqvist, Teo Mora, Eduardo Sáenz de Cabezón

Monday, July 17

Build. 34, 3d floor, Lecture Hall "Aula III"

14:00 – 15:00 **Sihem Mesnager**
A breakthrough concerning the solution of a famous equation on finite fields and its impacts in the context of S-boxes in symmetric cryptography

15:00 – 15:30 Rodrigo Iglesias, **Matthias Orth**, Eduardo Sáenz-de-Cabezon, Werner M. Seiler
A new view on the Rees algebra of a monomial plane curve parametrization

15:30 – 16:00 Coffee Break

16:00 – 16:30 **Cristina Bertone**, Francesca Cioffi, Matthias Orth, Werner M. Seiler
Marked bases for some quotient rings and applications - part I

16:30 – 17:00 Cristina Bertone, **Francesca Cioffi**, Matthias Orth, Werner Seiler
Marked bases for some quotient rings and applications - part II

17:00 – 17:30 Philippe Gimenez, Diego Ruano, **Rodrigo San-Jos'e**
Vanishing ideals and evaluation codes

17:30 – 18:00 **Viktor Levandovskyy**
Letterplace: theory, technology, and implementation

Tuesday, July 18

Build. 34, 3d floor, Room 3/40

09:00 – 09:30 **Filip Jonsson Kling**, Samuel Lundqvist, Lisa Nicklasson
On binomial complete intersections

09:30 – 10:00 **Lisa Nicklasson**
Pinched Veronese algebras

10:00 – 10:30 **Victor Ufnarovski**, Erik Kennerland, Anna Torstensson
Almost monomial subalgebras of MK[x] and their LAGBI bases

10:30 – 11:00 **Discussion**

Tuesday, July 18

Build. 34, 3d floor, Room 3/40

16:00 – 16:30 **Yosuke Sato**, Ryoya Fukasaku
On simplification of comprehensive Gröbner systems

16:30 – 17:00 **Tateaki Sasaki**
Term elimination sequence and removal of extraneous factors in two-polynomial systems

17:00 – 17:30 **Shinichi Tajima**, Katsusuke Nabeshima
Testing tameness of a complex polynomial map via comprehensive Gröbner systems

17:30 –18:00 **Katsusuke Nabeshima**, Shinichi Tajima
Primary decomposition via algebraic local cohomology with tag variables

18:00 – 18:30 **Deepak Kapur**
A Gröbner basis as a combination of congruence closures

Schedule for Algebraic and Algorithmic Aspects of Differential and Integral Operators Session

Organized by Moulay Barkatou, Thomas Cluzeau, Clemens Raab, Georg Regensburger

Tuesday, July 18

Build. 34, 3d floor, Lecture Hall "Aula IV"

09:00 – 09:30 **Mohamed Barakat**
Doctrine specific ur-algorithms

09:30 – 10:00 **Vladimir V. Bavula**
The most general theory of one-sided fractions

10:00 – 10:30 **Manfred Buchacher**
The Newton-Puiseux algorithm and effective algebraic series

10:30 – 11:00 **Alexander Levin**
New dimension polynomials and invariants of inversive difference-differential field extensions

Tuesday, July 18

Build. 34, 3d floor, Lecture Hall "Aula IV"

14:00 – 14:30 **Cyrille Chenavier**, Thomas Cluzeau, Alban Quadrat
Computation of Koszul homology and application to involutivity of partial differential systems

14:30 – 15:00 **Clemens Hofstadler**, Clemens G. Raab, Georg Regensburger
A semi-decision procedure for proving operator statements

15:00 – 15:30 **Sette Diop**
A differential algebraic approach of systems theory

15:30 – 16:00 Coffee Break

16:00 – 16:30 **Shaoshi Chen**, Hao Du, Hui Huang, Ziming Li
Hypergeometric creative telescoping (online)

16:30 – 17:00 **Li Guo**, Yunnan Li, Yunhe Sheng, Rong Tang
Crossed homomorphisms and Cartier-Konstant-Milnor-Moore theorem for difference Hopf algebras (online)

17:00 – 17:30 **Alexei Cheviakov**
Approximate symmetries and conservation laws and their applications to PDEs (online)

17:30 – 18:00 **Antonio Jiménez-Pastor**
Difference-differential polynomials in SageMath

Wednesday, July 19

Build. 34, 3d floor, Lecture Hall "Aula IV"

16:00 – 16:30 Thomas Cluzeau, **Camille Pinto**, Alban Quadrat
Towards an effective integro-differential elimination theory

16:30 – 17:00 **Franz Winkler**
Symbolic solutions of differential equations

17:00 – 17:30 Thieu N. Vo, **Yi Zhang**
Rational solutions of first-order algebraic ordinary difference equations

17:30 – 18:00 **Viktor Levandovskyy**
On an interplay of computer algebra and ring theory

Thursday, July 20

Build. 34, 3d floor,Room 3/40

09:00 – 09:30 **Sebastian Posur**
An abelian ambient category for behaviors in algebraic systems theory (online)

Contents

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

Computer Algebra Systems and Interval Methods

Computer Algebra Applications in the Life Sciences

Computational Differential and Difference Algebra and its Applications

Algebraic Geometry from an Algorithmic Point of View

Effective Ideal Theory and Combinatorial Techniques in Commutative and Non-Commutative Rings and Their Applications

Algebraic and Algorithmic Aspects of Differential and Integral Operators

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17 – 21, 2023
"Invited Speaker"

Wolfram's Vision for Unified Computation

Jon McLoone [jonm@wolfram.com]

Wolfram Research Europe

The presentation will delve into the philosophy that has been the driving force behind the development of Wolfram Language over the past 35 years, while also shedding light on its current priorities. Additionally, the talk will explore how this philosophy has been applied to the integration of significant advancements in generative AI.

To illustrate this alignment, examples from the latest Mathematica 13.3 will be shown.

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17 – 21, 2023
"Invited Speaker"

Theoretical and Numerical Analysis of Singular Initial and Boundary Value Problems

Werner M. Seiler [seiler@mathematik.uni-kassel.de]

Kassel University, Germany

We consider quasilinear ordinary differential equations both theoretically and numerically. We call an initial or boundary value problem singular, if at the corresponding point the coefficient of a derivative of highest order vanishes. In such a situation, the well-known existence and uniqueness theorems cannot be applied and also classical numerical integrators typically break down in the vicinity of such a singularity. Using a geometric view of a differential equation as a submanifold in a suitable jet bundle, we define an explicit dynamical system on this submanifold and relate questions of existence, (non)uniqueness and regularity of solutions to standard problems in dynamical systems theory. Furthermore, this point of view leads in a straightforward manner to a simple and robust numerical approach to singular initial and boundary value problems. As examples, we will consider classical equations like Lane-Emden or Thomas-Fermi and show how the for applications relevant initial and boundary value problems can be solved in a few lines of Maple code.

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17 – 21, 2023
"Invited Speaker"

Recent Symbolic Computation Developments in Mathematica

Adam Strzebonski [adams@wolfram.com]

Wolfram Research, USA

In this talk a general overview of recent improvements in Mathematica symbolic computation capabilities will be presented and some of the improvements will be discussed in more detail. We will focus on new methods for finding exact solutions of systems of equations and inequalities and for solving exact optimization problems, performance improvements in polynomial algebra functions, and on new functionality for computation over finite fields.

Applications of Computer Algebra – ACA 2023
July 17-21, 2023
Session on *"Computer Algebra in Education"*

Assessment of students' knowledge and abilities in undergraduate mathematics

Elena Varbanova[1]***, Stoyan Kapralov***[2]***, Stanislav Simeonov***[3] [elvar@tu-sofia.bg]

[1] Faculty of Applied Mathematics and Informatics, Technical University of Sofia, Sofia, Bulgaria
[2] Technical University of Gabrovo, Gabrovo, Bulgaria
[3] University "Prof. Dr Asen Zlatarov", Burgas, Bulgaria

In memory of Eugenio Roanes-Lozano

In the triad Teaching-Learning-Assessment (TLA) the components are to be considered in tandem, not standalone. The activities are to be interrelated, because what gets assessed is what gets taught. That is why we need to focus on: purposeful Teaching, purposeful Learning and purposeful Assessment. A TLA process could help the students build habits and qualities of mind that are useful for the real life and, above all, for their work.

Typically, teachers ask the students increasingly challenging questions to test their comprehension of a given material. In the textbooks, the most common verbs are find, determine, calculate, solve, explore. These abilities show that the student has accomplished the goal "Remember, Understand and Apply" (in Blooms taxonomy), i.e. Lower Order Learning (LOL); the latter are really necessary and important and have to be assessed. However in technology enriched teaching-learning environment there are opportunities to interpret this goal and change the way of its accomplishment. Higher Order Learning (HOL: development of abilities to analyze, synthesize, create) is to be also achieved and assessed. Care must be taken to changes: the things we think are changing aren't always what's changing.

The students have to learn certain things, to achieve learning outcomes, as well as to learn how to learn. New professions require not only knowledge and skills, but also logical, critical and creative thinking. The student has to build up as well the habit to do things in sequence in order to develop an organized and disciplined mind. The assessment of students' knowledge and abilities has to assure the accomplishment of these qualities. Here we share thoughts and experience in this direction.

Using a CAS any Taylor polynomial of interest can be obtained. Then instead of its determination further questions for testing the deepness of students' knowledge of this concept can be set up. For instance, consider the following tasks.

Task 1. Given the 5th degree Taylor polynomial $T_5(x) = \frac{x}{2} + \frac{x^2}{8} + \frac{x^3}{24} + \frac{x^4}{64} + \frac{x^5}{160}$ at the point $x_0 = 0$ of the function $f(x) = \ln \frac{2}{2-x}$.

(a) Show that the first term is correct.

(b) Calculate an approximation of $f(0.5)$ (or of $\ln \frac{4}{3}$) using the second degree Taylor polynomial $T_2(x)$ at the point $x_0 = 0$.

(c) Evaluate $f^{(5)}(0)$.

Task 2. The function $f(x) : R_+ \to R_+$ satisfies the following conditions:

$$f(4) = 2, f'(4) = 0.25, f''(x) = -\frac{0.25}{x\sqrt{x}}.$$

(a) Find the polynomial of Taylor of 3rd degree $T_3(x)$ of $f(x)$ at the point $x_0 = 4$.

(b) Calculate an approximation of $f(4.2)$ using the second degree Taylor polynomial $T_2(x)$ at the point $x_0 = 4$.

(c) Determine the function $f(x)$.

The aim of such kind of questions is to help students consolidate key knowledge about Taylor polynomials: their construction, their applications: for calculating values of functions, for solving approximately integrals and differential equations. The solution also aims at HOL and development of the habit to solve problems not just any how, to work (consequently, perform any activity) smarter not harder. In the presentation the approach to the solution of the above tasks will be considered.

In case of Fourier series similar questions can be formulated. When the student is checking up, for instance, the correctness of a term he/she develops the habit to control the results using different prototypes (analytical, numerical, graphical) including those obtained by application of software.

Task 3. Given the Fourier series $f(x) = \frac{\pi}{2} + \frac{4}{\pi}\cos x + \cdots + a_n \cos(nx) + \ldots$ for the periodic function $f(x) = \begin{cases} \pi + x, & -\pi \leq x \leq 0 \\ \pi - x, & 0 \leq x \leq \pi \end{cases}$, $f(x + 2\pi) = f(x), \ x \in R.$

Show that the second term is correct. Sketch the graph of f and justify the form of the series.

CASs allow to formulate questions based on visual information.

Task 4. The area D is bounded by the curves $y = 9 + 3x$ and $y = 9 - x^2$ (Fig. 1). Describe D in terms of double inequalities in two ways. Calculate the integral $\iint\limits_D dydx$ and interpret the result.

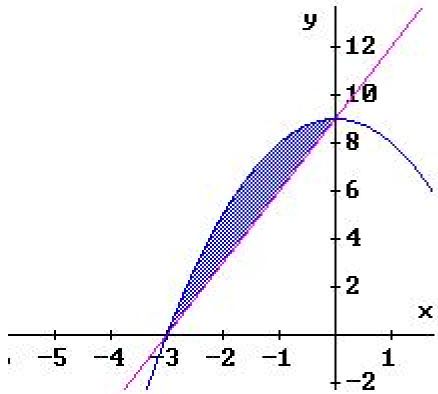


Fig. 1

"Work smarter, not harder" is related to effective solutions. Asking right questions ensures effective learning. In connection to effectiveness the following cases will be considered in the presentation.

1) Evaluate the second order partial mixed derivative of the function

$$f(x, y) = \ln(2x + 5) - 2x\arctan(2x) + e^{5y} + \sin(xy) + 24 \text{ at the point } P\left(\frac{\pi}{2}, 1\right).$$

2) Solve: $\displaystyle\int \frac{\mathrm{d}x}{x\ln(x)}$; $\displaystyle\int x\sqrt{16 - x^2}\mathrm{d}x$; $\displaystyle\int_0^1 \sqrt{1 - x^2}\mathrm{d}x - \int_0^{0.5} \sqrt{\frac{1}{4} - x^2}\mathrm{d}x$;

$$\int_{-0.5}^{0.5} (12x^3 + x\cos(x) - 6\pi\cos(3\pi x))\mathrm{d}x.$$

By the choice of an approach to the solution the basic question is whether to apply a method if the solution can be obtained by direct application of definitions, properties or/and graphical images.

Mathematics and computer science education is of great importance to society. Any activity to stimulate and provoke the interest of young people to these fields will be for the benefit of society. This would produce added value to this education. The second author of this paper proposed the idea of organizing national student contest in mathematics with application of CASs. He shared it with university teachers keen to implement CASs in the teaching-learning process. As a result of teachers' and students' enthusiasm the experimental competition in Computer Mathematics took place in 2011 in Bulgaria [1]. The 9th edition of CompMath was held in October 2022.

It has to be mentioned that in the past several years Geo-Gebra is intensively used at Bulgarian math high schools. Advanced students and students who prefer doing mathematics in technology-supported environment are the majority of participants in this competition. All they need to be stimulated by additional activities at the universities: establishment of initiatives such as informal education, visiting lecturers - distinguished professionals in computer mathematics and computer science, clubs for exchange of ideas and experience. Based on their achievements they need to be advised to acquire additional learning material, so that to develop their full potential.

CompMath is now a traditional annual forum for students at Bulgarian universities. It proved to be useful for stimulating students' interest in mathematics and the opportunities of CASs for solving both theoretical and applied problems. It helps to create new as well as best practices in mathematics education: they could serve as models for suitable purposeful problems and assessment criteria.

The participants in the CompMath are given 30 mathematical problems to be solved within four hours. Based on their bachelor degree program they are divided into two groups:

- Group A: Mathematics, Informatics, Computer Science;

- Group B: Engineering, Natural Sciences.

All topics from the mathematics courses are covered. The students solve the problems in different ways depending on the level of their mathematical knowledge and programming skills. In the presentation some interesting problems and solutions created by participants will be demonstrated [2]. Mathematica, Maple, Maxima, Derive and MATLAB are mostly used in CompMath.

Acknowledgements
This research was funded in part by the European Regional Development Fund through the Operational Program "Science and Education for Smart Growth" under contract UNITe No BG05M2OP001–1.001–0004 (2018–2023).

Keywords
undergraduate mathematics, CASs, assessment, competition in computer mathematics

References
[1] COMPMATH, `www.compmath.eu`, Accessed 20/05/2023.
[2] S. KAPRALOV, S. BOUYUKLIEVA, P. KOPANOV, Compmath 2018 – The Seventh Student Olympiad in Computer Mathematics. In *Proceedings of the EDULEARN19 Conference*, 9964-9970, Palma, Mallorca, Spain, 1st-3rd July 2019, ISBN: 978-84-09-12031-4.

Applications of Computer Algebra – ACA 2023
July 17-21, 2023
Session on *“Computer Algebra in Education”*

Online drills created by extended CindyJS and scoring them with Maxima

Setsuo Takato[1], ***Hideyo Makishita***[2] [takato@jcom.home.ne.jp]

[1] KeTCindy Center, Magnolia Inc., Kisarazu, Japan
[2] Department of Civil Engineering, Shibaura Institute of Technology, Tokyo, Japan

KeTCindy is a system to produce various graphics for LaTeX documents easily and interactively. It uses dynamical geometry software Cinderella as its GUI, and outputs TeX graphical codes such as Tpic, pict2e and Tikz. Actually, KeTCindy is a collection of functions described by Cindy Script, a generic programming language. The first author developed KeTCindy to input fine figures easily in the printed materials to be distributed in Mathematics classes[1]. Actually, not only the first but the second author utilizes KeTCindy to produce various geometric figures appeared in ‘wasan’, Japanese mathematics which was developed in Japan during the Edo period. Anyone can dowload KeTCindy package freely from CTAN(Congressive TeX Archive Network)
`https://ctan.org/pkg/ketcindy`,
or directly from
`https://github.com/ketpic/ketcindy`,
which one can search with the keyword ’ketcindy’.

KeTCindy can produce various kind of figures. Moreover it can call Maxima, C and R from the inside, where C is used to speed up hidden line removal which is important to create figures of 3d surfaces for printed materials. In 2014, Prof. Richter Gebert’s group in Technische Universität München developed CindyJS,
`https://cindyjs.org`
which is a web framework almost compatible with Cinderella. CindyJS produces HTML files with small size, about 20KB or so, but it might be a little insufficient to create various kind of web materials used in mathematics classes. So we developed KeTCindyJS which supports the use of some functions of KeTCindy with those of CindyJS. The steps are as follows.

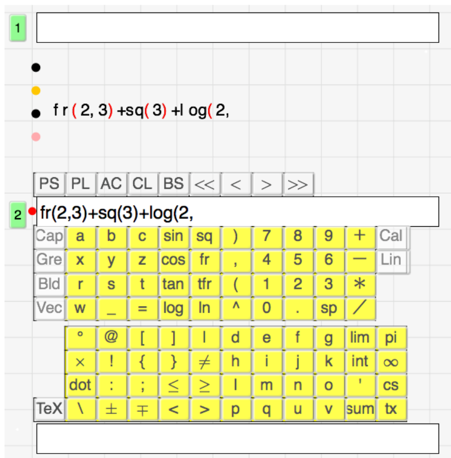
1. Export the HTML from Cinderella with pressing the button.
2. Press button ‘KeTJS’ in the KeTCindy file

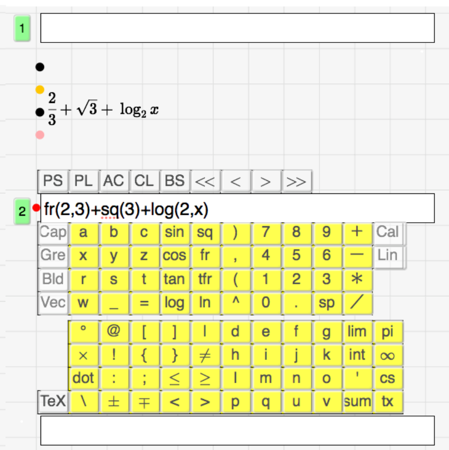
The size of the body HTML file is only 150KB and the size of libraries of KaTeX and CindyJS are 1.5MB, so totally less than 2MB. One can see the various samples in
`https://s-takato.github.io/ketcindysample/`.

During the pandemic, students and teachers were forced to web learning and teaching. In mathematics classes, to exchange questions and answers with formulae became a big problem. It would be rather easy for teachers to distribute questions, but it is much more difficult for students to send their answers and for teachers to collect/score them. The hard part for students is to write and send mathematical formulae with two-dimentional structure. So first, we set rules for one-dimensional expression.as follows:

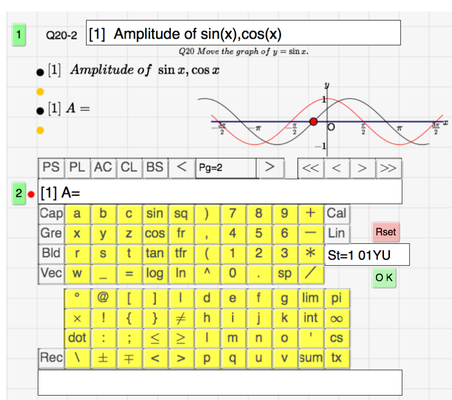
`fr(a,b)` for $\frac{a}{b}$, `sq(a)` for $\sqrt{a}$, `sin(2,x)` for $\sin^2 x$, `log(10,x)` for $\log_{10} x$, ...
Next, we developed an HTML application `KeTMath` using KeTCindyJS. It shows two-dimentional expressions when students input one-dimentional ones.

Remark: KeTMath is available with student's smartphone.





Moreover, we have developed KeTMath Learning Management System(KeTLMS). With this and with also a regular platform such as Google Classroom, Teams, Moodle and so on, teachers can send text-based questions, collect text-based answers and score them with Maxima.



Keywords
LaTeX, Maxima, KeTCindy

References

[1] S. TAKATO; A. MCANDREW; J.A. VALLEJO; M. KANEKO,Collaborative use of KeTCindy and free Computer Algebra Systems. *Mathematics in Computer Science* **11**, 503–514 (2017).

Applications of Computer Algebra – ACA 2023
July 17-21, 2023
Session on *Computer Algebra in Education*

ChatGPT excels in medicine but falters in basic algebra

Eli Bagno, Thierry Dana-Picard, Shulamit Reches

[ndp@jct.ac.il,bagnoe@g.jct.ac.il,shulamit.reches@gmail.com]

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

In memoriam of Eugenio Roanes-Lozano.

Lavoie [6] showed that the introduction of calculators in the classroom is a revolution similar to the switch from writing with a goose feather to writing with an iron quill. From time to time, new technologies appear in the world. Plotters, calculators, symbolic calculators, handheld devices, and more advanced Computer Algebra Systems. It is common sense that all these technologies enter the world of education. In particular, Engineering Education must involve various technologies in the courses, depending on the topics. An important reason is that the students have to develop a good literacy in technologies that they will use in their professional life. Moreover, because of the frequent development of new technologies, students have to acquire learning skills, which will be useful for lifelong learning.

Jerusalem College of Technology is an institution of Higher Education mostly devoted to High-Tech Engineering. Because of the large number of groups for every basic course, coordinators have to be appointed for these courses; the structure of the work is explained in [3]. Two of the authors are the coordinators of the two courses in Linear Algebra for engineers, and the other one is a teacher in the course . Every year, about seven hundred students are involved, divided into about ten lecture groups and more for practice sessions. This model has been developed at JCT for more than a decade [3], with continuous improvements, most of them allowed by technology. Recently a new technology, based on AI, has been released: ChatGPT.

ChatGPT is an impressive natural language processing tool that has made significant strides in recent years. It is capable of performing various tasks such as language translation, text summarizing, and even generating coherent and plausible stories. However, ChatGPT's abilities and limitations (see [2]) in mathematical problem-solving have to be thoroughly explored.

Our talk aims to examine ChatGPT's aptitude in mathematical problem-solving and the extent to which it can solve various math problems. Additionally, we will also analyze the limitations of ChatGPT in math and the potential for future advancements in this field[1].

ChatGPT has been tested for numerous possible applications in medicine, and its affordances have been analyzed; the success percentage is noticeable, but full success has yet to be achieved. [4]. A further remark about this software addresses the importance of communication using natural language [5]. This remark is of the utmost importance for us as educators. It has (almost) always been taken into account by software developers: generally, the syntax of commands in a Computer Algebra System is close to the way it would have been worked out by hand.

In this talk, we report on the first steps of ongoing research, which analyzes which benefits the teachers and the students can have from this technology in Linear Algebra. We elaborate also on some points from [9]. In particular, we show:

- Exercices in High-School algebra for which ChatGPT provides an accurate answer: elementary systems of linear equations;
- Examples in basic Undergraduate Linear Algebra where the system gives a correct answer;
- Examples in basic Undergraduate Linear Algebra where ChatGPT contradicts itself. Here we could identify problems mixing the inaccuracy of algebraic computations together with problems with recognition of what a set is.

In the last two cases, we tried to "teach" the system and made experiments using independent computers, in order for the system not to identify the user.

A complex instrumental genesis is at work [1, 7]: the teachers have to undergo such a process, and the AI-system too!

An analysis of the needed orchestration [8] with students is on its way also. Artigue [1] mentions that the implementation of a new technology depends on the "institutional culture". We are aware that some institutions in the world have already decided on the prohibition of using ChatGPt. Such a prohibition has been issued in Italy for the entire country, and cancelled a couple of weeks later with limitations. Our first results show that a more positive approach can be adopted. In particular, we identified that the system begins often by writing the definitions of the involved mathematical objects, an attitude that we try to educate our students.

Keywords
ChatGPT, Linear Algebra, Instrumental Genesis, limitations

Acknowledgment: The second author is partially supported by the CEMJ Chair, JCT.

[1]This paragraph is a slightly modified version of an answer given by ChatGPT. It shows that, as far as text is concerned, things are acceptable. In our talk, we address mathematical issues.

References

[1] M. Artigue, *Learning Mathematics in a CAS Environment*, The Genesis of a Reflection about Instrumentation and the Dialectics between Technical and Conceptual Work, International Journal of Computers for Mathematical Learning 7(3), 245–274 (2002).

[2] A. Azaria, *ChatGPT Usage and Limitations*, available: `10.13140/RG.2.2.26616.11526`, (2022).

[3] Th. Dana-Picard, I. Kidron, M. Komar and J. Steiner, ICT-aided engineering courses: a multi-campus course management, *European Journal of Engineering Education*, 31 (4), 373-381 (2006)

[4] Editorial, *Will ChatGPT transform healthcare?*,Nature Medicine 29, 505–506 (2023).

[5] J. Homolak, *Opportunities and risks of ChatGPT in medicine, science, and academic publishing: a modern Promethean dilemma*, Croatian Medical Journal 64(1), 1–3,doi: `10.3325/cmj.2023.64.1` (2003).

[6] P. Lavoie, *Contribution á une histoire des mathématiques scolaires au Québec*, l'arithmétique dans les écoles primaires (1800-1920), Thése de doctorat, Faculté des sciences de l'éducation, Université de Laval, Québec (1994).

[7] P. Rabardel, *From artefact to instrument interacting with Computers* 15(5), 641–645 (2003).

[8] L. Trouche, *Managing the Complexity of Human / Machine Interactions in Computerized Learning Environments: Guiding Students' Command Process through Instrumental Orchestrations*, International Journal of Computers for Mathematical Learning 9(3), 281–307 (2004)

[9] Z. Zachary, A. Pardos and S. Bhandari, *Learning gain differences between ChatGPT and human tutor generated algebra hints*, arXiv:2302.06871, (2023).

Applications of Computer Algebra – ACA 2023
July 17-21, 2023
Session on *"Computer Algebra in Education"*

Orthogonal Matrices: Third Time Around

Johannes Middeke*[1], *David J. Jeffrey*[1], *Aishat Olagunju `[djeffrey@uwo.ca]`

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

This presentation reflects new ideas about a topic which has been discussed at previous ACA conferences. Orthogonal matrices Q are defined by $QQ^t = dI$ where Q^t is the transpose, and I is the identity matrix with $d \neq 0$. Orthonormal matrices denote the special case $d = 1$. In addition to the important role they play in applications, such as the QR decomposition, orthogonal matrices are also useful to instructors in Linear Algebra and multivariable calculus. For example, if an instructor wants to create a problem in which lines intersect at a given angle, then one way to do this is to create the problem in a simple configuration and then use an orthogonal matrix to transform the problem to a more complicated one. Thus, the lines $L_1 = r\langle 1, 0, 0\rangle, L_2 = s\langle 1, 1, 0\rangle, L_3 = \langle 2, 0, 0\rangle + t\langle 0, 1, 0\rangle$ form a simple triangle, but after multiplying by Q, they still form a triangle with the same angles, but are now shifted and rotated in space.

For pedagogical reasons, it is very helpful to students if Q matrices have rational elements. In this talk, we shall discuss various ways in which orthogonal and orthonormal matrices with purely rational entries can be computed. Our aim is to create a repository of rational orthogonal matrices for instructors to use when creating examples and exercises. Access will be free and open.

The first approach utilises an exhaustive search. Since the columns of any rational orthonormal matrix must form a Pythagorean n-tuple, we start by generating the list of all primitive Pythagorean n-tuples where the entries are below a certain size. We then combine the tuples until we have found an orthonormal matrix. (Note that we only need to find $n - 1$ columns in this way; the n-th column is then uniquely determined and can be computed by other means.) The benefit of this method is that we gain tight control over the sizes of the matrix entries, which is helpful for generating and ordering our open database of orthogonal matrices. A repository is more useful if the entries are not randomly presented.

A second method is based on a result by Cayley [1]: If A is a skew-symmetric rational matrix, then $(I - A)^{-1}(I + A)$ will be orthogonal; and all rational orthogonal matrices which do not have 1 as an eigenvalue can be obtained in this way. In [2], Liebeck and Osborne have shown that every orthogonal matrix can be transformed into an orthogonal matrix for which 1 is not an eigenvalue through multiplication of its rows by ± 1. Hence, Cayley's formula can be used to obtain all orthogonal matrices. We analyse some interesting patterns which arise from the use of this method.

Finally, rational orthonormal matrices of higher dimension can be generated by composing smaller orthonormal matrices. For example, it is well known (see, e. g., [3]) that the Kronecker product of orthonormal matrices is itself orthonormal. Also, block diagonal matrices where the blocks are orthonormal will themselves be orthonormal. If we multiply these block diagonal matrices by random permutations, it becomes easy to generate orthonormal matrices with a predefined degree of sparseness.

Keywords
Orthogonal matrices, Pythagorean numbers, undergraduate education

References
[1] F. GANTMACHER, *Matrizentheorie*, Springer-Verlag, Berlin Heidelberg, 1986.
[2] H. LIEBECK; A. OSBORNE, The Generation of All Rational Orthogonal Matrices, *American Mathematical Monthly*, **98**(2), 131–133 (1991).
[1] J. E. GENTLE, *Matrix Algebra*, Springer, New York, 2017.

Applications of Computer Algebra – ACA 2023
July 17-21, 2023
Session on *"Computer Algebra in Education"*

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

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

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

In memory of Eugenio Roanes-Lozano

At ETS, CAS technology is mandatory since 1999 and TI-Nspire technology is used campus wide since 2011 (both calculator and software). The talk will be the third of a series about how technology has changed the way we teach mathematics to future engineers. First, let us recall what we did in the last two ACA conferences.

For the online 2021 Athens conference, a third degree polynomial equation was chosen. Newton's method was applied and animated in order to find the roots. Cardano's formulae were deduced using CAS manipulations. We showed why trigonometric substitutions are a better choice when all roots are real.

For the 2022 hybrid Istanbul conference, complex analysis was chosen. We visualized the complex roots of a polynomial using 2D and 3D plots using TI-Nspire CAS. We showed how Laurent series, residue integration techniques and numerical line integrals can be combined to verify some answers. And how the Maple built-in Rieman Zeta function allows us to observe some non trivial zeros of $\zeta(s)$.

For this in person 2023 Warsaw conference, ODEs and real analysis are chosen. The examples listed below are interesting for a student to explore when a CAS handheld is available during the classroom. Using some popular computer algebra systems, the examples will be performed live during the talk.

- Heavy computations are often required in ODEs application problems, so using a CAS has always been natural. But theoretical results (namely the existence and uniqueness of solutions) can benefit from CAS computations and graphic facilities. It is quite interesting to look at the answer provided by popular CAS when solving

  $$\frac{dy}{dx} = \frac{4y}{x^2 - 9}, \quad y(a) = b\,.$$

  For some initial values, hidden complex numbers can appear on the screen due to cubic roots. This is a good opportunity to recall the domain of a solution. The textbook [1] is famous for this : the authors took special care of linearity and effects of parameters on solutions instead of listing many tricks for solving different ODEs.

- Engineering students rarely use mathematical analysis. Pointwise convergence of series of functions is not an important part of their curriculum. At ETS, the differential equations course has been updated recently (see [2] where you can download my colleague Gilles Picard's *Volume* 2). Taylor series method for solving ODEs along with numerical methods are used for linear variable coefficients second order ODEs. Example : without technology, one can find a series solution $y(x) = \sum_{n=0}^{\infty} a_n\, x^n$ for the problem $(x^2+1)\, y'' - 3y' + y = 0, y(0) = 1, y'(0) = -1$. But when the following recurrence formula will be found, we will need a machine to compute the coefficients :

$$a_n = \frac{3(n-1)\, a_{n-1} - (n^2 - 5n + 7)\, a_{n-2}}{n(n-1)},\ n \geq 2.$$

  Then if you want to compute **with accuracy** the value of the solution at some point x_0 of the interval of convergence, you need to use a partial sum of the form

$$so(p) = \sum_{n=0}^{p} a_n\, x_0^n.$$

  Finally, a numerical first-order system ODE solver can validate the answer.

- Equation solving can benefit from CAS graphical capabilities. A simple example as solving $x^x = a$ for different values of the parameter a can easily force the students to use calculus and get to know the LambertW function!

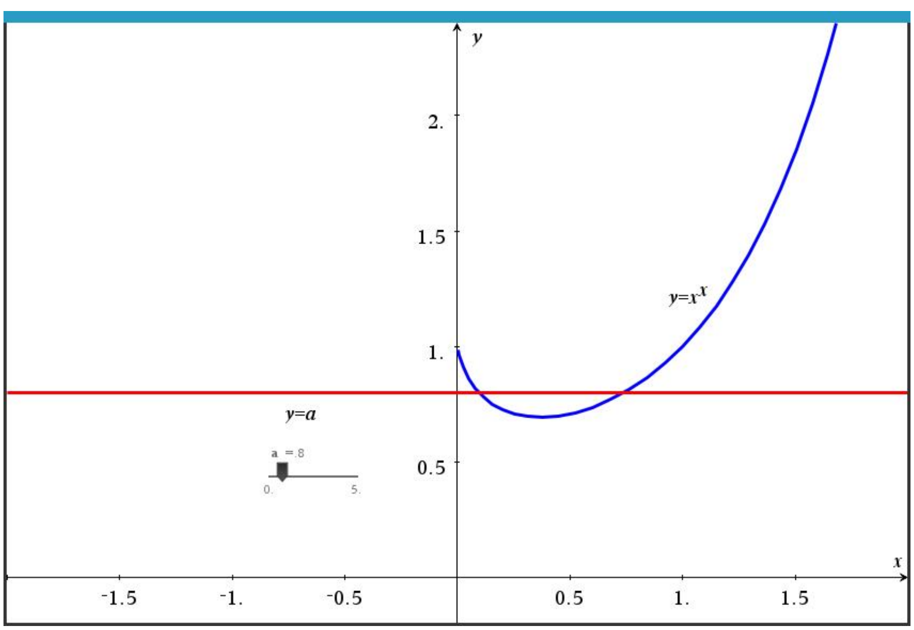


Figure 1: Horizontal line intersecting the curve x^x

References

[1] KOSTELICH, ERIC J.; ARMBRUSTER, DIETER, *Introductory Differential Equations. From Linearity to Chaos*. Addison Wesley, 1997.

[2] https://luciole.ca/gilles/mat265/.

.

Applications of Computer Algebra – ACA 2023
July 17-21, 2023
Session on *"Computer Algebra in Education"*

Surfaces and their Duals

Josef Böhm[1] [nojo.boehm@pgv.at]

[1]DUG and ACDCA, Austria

In memory of Eugenio Roanes-Lozano

Recently, I found among my many papers a one-page article about *Dual Surfaces*, written by Dr. Richard Morris, Liverpool University, which appeared in the Maths&Stats journal, which was published for several years by the University of Birmingham. It must have been before 2000 because I could not find the article in the MSOR Maths&Stats archives : see [1] and [2]. Dr. Morris wrote: *The dual of a surface is the set of planes tangent to the surface*. The mapping works as follows. Any plane $a\,x + b\,y + c\,z = d$ can be interpreted as a point (a, b, c, d) in RP^3. Morris performs a projection of these points into $\mathbb{R}^3$ using the map

$$(a, b, c, d) \to \left(\frac{a}{c}, \frac{b}{c}, \frac{d}{c}\right).$$

Some pictures in a low quality were included. This was all!

I will show how to perform this mapping using *DERIVE* and TI-Nspire CAS as well and present various surfaces together with their duals. Cusps appear and we can ask where they are coming from? Then I will vary the mapping followed by parameter curves and their duals. More questions come up, like *How does the dual of a dual look like?* This would be a nasty and boring calculation done by hand, but using a CAS this becomes possible. Finally, I don't raise the problem in a higher dimension – as generalisation usually works – but do it the reverse way: I make a step down and try to find the dual of a plane curve. Again cusps appear. Where do they come from? Preparing this presentation I did some internet research – and I was lucky enough to find in [3] another much more extended paper published by Morris also in 2002 – which provided more insight for the properties of the duals. So, this short article of Dr. Morris from 2002 kept me busy some time and brought a lot of pleasure and surprise into my mathematical life which I would like to share with an audience. I'll show among others a dual with cuspidal edges (Fig 2), how they can be derived and from where they are coming from in the base surface (Fig 1). The references could be accomplished with [4].

Keywords
Dual surfaxes, Mappings, Gauss Curvature, Graphic Representations

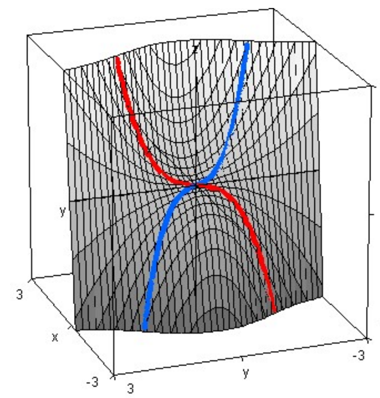


Figure 1: Base surface

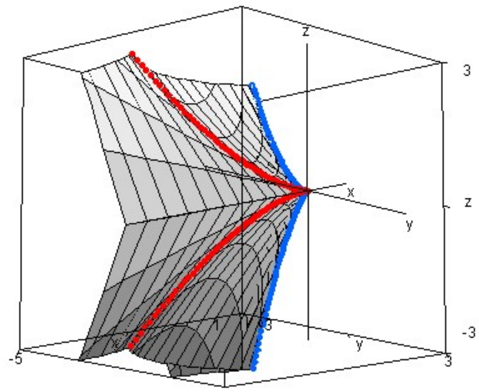


Figure 2: Dual with cuspidal edges

References

[1] `https://journals.gre.ac.uk/index.php/msor/issue/archive`

[2] `https://icse.xyz/mathstore/node/568-2.html`

[3] `https://www.singsurf.org/papers/dual/dual.pdf`

[4] Alfred Gray, *Differentialgeometrie*, Spectrum 1994.

Applications of Computer Algebra – ACA 2023
July 17-21, 2023
Session on *"Computer Algebra in Education"*

Rubi gems

David J. Jeffrey[1], ***Albert D. Rich*** [djeffrey@uwo.ca]

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

1 Abstract

The Rule-Based Integration project (Rubi) has been under continuous development since 2008. The current publicly available release is version 4.16.1.0 available at [1]. Active development of Rubi's database of rules has continued unabated since that version. This report selects a few of the recent additions to Rubi, and describes some of the processes that help direct the research into new rules.

We recall that while the primary aim of Rubi is to evaluate indefinite integrals using a rule-based paradigm, an important aspect of this aim is that Rubi is not content to return *just any* expression that is a valid integral, but aims to return *the best* or *optimal* integral expression.

1.1 The best integral

How do we decide which of these integrals is better?

$$2\sqrt{2}\int \frac{t^2}{1+t^4}\,dt = \arctan\frac{-1+t^2}{\sqrt{2}\,t} - \operatorname{arctanh}\frac{\sqrt{2}\,t}{1+t^2}\,, \tag{1}$$

$$= \arctan(\sqrt{2}\,t+1) + \arctan(\sqrt{2}\,t-1) - \operatorname{arctanh}\frac{\sqrt{2}\,t}{1+t^2}\,. \tag{2}$$

We shall discuss this question.

1.2 Some new trig integrals

One of Rubi's great strengths is special cases. The integral below is one special case of a general class. Using the rule for the general class results in a very long answer. In new Rubi, the special case is recognized and returned.

$$\int \frac{\sin(100x) + \sin(99x)}{\cos(100x) + \cos(99x)}\, dx = -\frac{2}{199} \ln \cos \frac{199x}{2} \; .$$

Keywords
Symbolic integration, rule-based systems, optimal expression analysis

References
[1] A. D. Rich, *Rubi (Rule-based Integrator)*,
https://rulebasedintegration.org/about.html

Applications of Computer Algebra – ACA 2023
July 17-21, 2023
Session on *Computer Algebra in Education*

Automated computation of geometric Loci in Mathematics Education

Thierry Dana-Picard[1], ***Tomas Recio***[2] [ndp@jct.ac.il,trecio@nebrija.es]

[1] Mathematics Department, Jerusalem College of Technology, Jerusalem,Israel
[2] Antonio de Nebrija University, Madrid, Spain

In memoriam of Eugenio Roanes-Lozano.

The computation of geometric loci is an important topic, both at High-School level and at undergraduate level. This topic has been explored for a long time [1,2]. Nevertheless, the goals and the methods which can be utilized with todays' tools are different. At undergraduate level, the dialog between Geometry and Algebra is fruitful [3, 5], but it is less relevant for High-School. For example, section 4.2 in [3] emphasizes the process of obtaining locus visualization (image, equation), and considers sophisticated examples, far from the contents of the pre-university education in most countries. Moreover, it does not develop the two steps that we consider more relevant when dealing with secondary education.

These steps will be the main points of attention in our contribution here:

- conjecturing the loci structure —and not only its equation or plot—
- and verifying the soundness of the conjecture—with automated reasoning tools.

In our contribution, we will argue how both tasks should be, in the educational context, the more relevant ones that students of today (or tomorrow) would have to learn. We exemplify these ideas with two examples:

1. Ptolemy's theorem;
2. a very simple, yet not obvious, locus, namely that of the vertex C of a triangle ABC, such that the medians from A to the midpoint of AC and from B to the midpoint of BC are perpendicular (Figure 1).

As an example of our disquisitions, let us mention that, in the second example, one immediate output of the exploration can be an equation for the desired geometric locus, but this equation

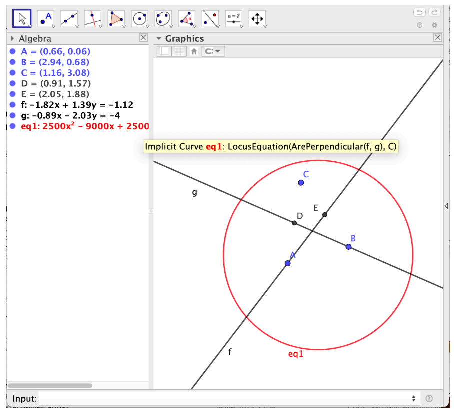


Figure 1: Automated determination of a locus

is only computed numerically, and it might be of little help for a High-School student searching for some geometric features (center, radius) of this locus. Moreover, the plotted circle is just a "shape", not a geometric object recognized by the software, and standard GeoGebra commands such as "Prove" (also available as a button) cannot apply to verify conjectures over this plot. Thus, students have to explore and confirm their conjectures with the use of more advanced tools offered by GeoGebra-Discovery [4] that provide an exact answer, and enable to determine "what is really" the desired locus, after implementing a "true' geometric construction of the circle, using plane transformations which have automated implementations in the software.

Keywords
Geometric Locus, GeoGebra-Discovery, Automated Proof

Acknowledgment: First author partially supported by the CEMJ Chair at JCT. Second author supported by grant "Mathematical Visualization: Foundations, Algorithms and Applications" (PID2020-113192GB-I00), from the Spanish MICINN.

References

[1]J. Blazek; P. Pech, Searching for loci using GeoGebra, *International Journal for Technology in Mathematics Education* **27**, 143–147 (2017)
[2] F. Botana, M. Abánades, Automatic Deduction in (Dynamic) Geometry: Loci Computation, *Computational Geometry* **47 (1)**, 75-89 (2014).
[3] Th. Dana-Picard, Computer assisted proofs and automated methods in mathematics education. In: *Theorem Proving Components for Educational Software 2022 (ThEdu'22)*, J. Marcos, W. Neuper and P. Quaresma (eds.), 2–23. EPTCS 375, 2023, `doi:10.4204/EPTCS.375.2`
[4] Z. Kovács , T. Recio, Ph. Richard, S. van Vaerenbergh, M. Pilar Vélez, Towards an Ecosystem for Computer-Supported Geometric Reasoning, *International Journal of Mathematics in Science and Technology* **53 (7)** (2022).
[5] P. Pech, *Selected Topics in Geometry with Classical vs. Computer Proving*, World Scientific Publishers, 2007).

Applications of Computer Algebra – ACA 2023
July 17-21, 2023
Session on *"Computer Algebra in Education"*

GeoGebra Automated Reasoning Tools: why and how (to use them in the classroom)

***Zoltán Kovács*[1], *Tomás Recio*[2], *M. Pilar Vélez*[2]** [pvelez@nebrija.es]

[1] The Private University College of Education of the Diocese of Linz, Linz, Austria
[2] Escuela Politécnica Superior, Universidad Antonio de Nebrija, Madrid, Spain

In memory of Eugenio Roanes-Lozano

Dynamic Geometry (DG) systems have become quite popular for teaching purposes. Although initially characterized by the ability to drag geometric constructions while keeping the relations (perpendicularity, parallelism, etc.) established by the user among the involved geometric objects, some of these environments evolved to integrate a computer algebra system, so they should be better described as "dynamic mathematics" software. This is the case of GeoGebra[1], integrating the computer algebra system Giac. This has opened the possibility to translate algebraically the geometric relations between objects in a construction and, thus, to deal with computer algebra algorithms that allow the development of highly performing, mathematically rigorous (not just probabilistic or numerically approximate) Automatic Reasoning Tools (ART) on geometric statements. Thus, currently GeoGebra (and, for some advanced tools, the fork version GeoGebra Discovery[2]) already offers the user a rich variety of ART for tasks related to experimenting, discovering, and asserting:

- Automatically declaring the truth or failure of a given statement (`Prove` and `ProveDetails` commands),
- Automatically discovering how to modify a given figure so that a wrong statement becomes true (`LocusEquation` command, returning where to place some point on a construction so that a given property holds),
- Automatically discovering and returning a message with the properties holding among some selected pair of elements of the given figure (`Relation` command),
- Automatically discovering all statements (of a certain kind: lengths ratio, perpendicularity, etc.) holding true and involving a given element in a figure, selected/introduced by the user (`Discover`, `StepwiseDiscovery` command),

[1] `http://www.geogebra.org`
[2] `https://github.com/kovzol/geogebra/releases`

- Automatically discovering all statements of a certain kind involving “all” the elements of a given figure, see [3].

Unfortunately, the algebraic geometry nature of the algorithms behind these tools does not allow providing readable arguments justifying their outputs. Yet, we think that the universal accessibility and portability of GeoGebra; its worldwide diffusion, with more than 100 million users all over the world – especially in the educational field – requires the analysis and design of new approaches to teaching proof at secondary education level and beyond, because teaching geometry to students that have at their disposal powerful ART which they can apply to deal with geometric problems, cannot be a mere repetition of the traditional curriculum: teachers should learn about this technology and should explore its application in the classroom

As it was already noticed by Howson and Wilson, too long ago, in the publication known as Kuwait report [1]:

> “. . .today’s student may well be able to apply algebraic methods. . . The solution derived by applying a mechanical procedure may be less aesthetically satisfying than a geometrical one, but are there other objections to algebraic methods than that of aesthetics?”

As well as very recently in a paper by Hanna and Yan [2]:

> “It is perhaps too early for empirical studies of classroom experience using the enhancements to GeoGebra. In this respect the situation of GeoGebra is similar, but not identical, to that of proof technology in general. While it is reasonable to expect proof technology to foster students’ proving abilities, and there is certainly supporting anecdotal evidence, its potential advantages have not yet been systematically assessed. . . Theorem provers do provide a guarantee, as we have seen, but in the shape of a fully formal proof that may be unintelligible. . . This state of affairs is a challenge for educators. . . They also have reason to believe, based on the anecdotal evidence, that this new proof technology could turn out to be of great benefit in the classroom. . . The key is to make a start, beginning with exploratory studies of the potential of these new tools at both the secondary and post-secondary levels.”

Thus, the purpose of this talk is, firstly, to make a summary presentation of the abovementioned automated reasoning functions in GeoGebra, through some illustrative examples [3], [4]. Then we will focus on the proposal of diverse open-ended tasks, inspired in recent experiences ([5], [6], [7]) that have been developed with different kinds (secondary education, undergraduate or initial teacher training) of students, regarding the use of automated reasoning techniques, showing how these tools can be used within the educational context, helping students to develop “augmented intelligence” skills by reasoning in collaboration with the computer.

Acknowledgements: Authors are partially supported by grant PID2020-113192GB-I00 (Mathematical Visualization: Foundations, Algorithms and Applications) from the Spanish MICINN.

[3] `https://autgeo.online/ag/automated-geometer.html?offline=1`

Keywords
Automated reasoning in geometry, GeoGebra, Math instruction, Augmented intelligence

References

[1] G. HOWSON; B. WILSON, *ICMI Study series: School mathematics in the 1990's*. Cambridge University Press, 1986.
[2] G. HANNA; X. YAN, Opening a discussion on teaching proof with automated theorem provers. *For the Learning of Mathematics* **41**(3), 42–46 (2021).
[3] Z. KOVÁCS; T. RECIO; P.R. RICHARD; S. VAN VAERENBERGH; M.P. VÉLEZ, Towards an Ecosystem for Computer-Supported Geometric Reasoning. *International Journal for Technology in Mathematics Education (IJTMT)* **53**(7), 1701–1710 (2022).
[4] Z. KOVÁCS; J. YU, Stepwise discovery of geometrical knowledge in GeoGebra. *Proceedings of The 8th Czech – Slovak Conference on Geometry and Graphics 2022*, M. Lavicka, M. Chodorová, L. Rýparová, D. Szarková (eds.) Plzeň, 2022.
[5] T. RECIO; P.R. RICHARD; M.P. VÉLEZ, Designing tasks supported by GeoGebra Automated Reasoning Tools for the development of mathematical skills. *International Journal for Technology in Mathematics Education (IJTMT)* **26**(2), 81–89 (2019).
[6] J.M. FORTUNY; T. RECIO; P.R. RICHARD; E. ROANES-LOZANO, Análisis del discurso de los profesores en formación en un contexto de innovación pedagógica en geometría. *Annales de Didactique et de Sciences Cognitives* **26**, 195–220 (2021).
[7] A. HERRERO; T. RECIO; P. TOLMOS; M.P. VÉLEZ, From the Steam Engine to STEAM Education: An Experience with Pre- Service Mathematics Teachers. *Mathematics* **11**(2), 473 (2023).

Applications of Computer Algebra – ACA 2023
July 17-21, 2023
Session on *"Computer Algebra in Education"*

Orthogonal trajectories to isoptics of ovals

Magdalena Skrzypiec[1]***, W. Mozgawa***[2]***, A. Naiman***[3]***, P. Pikuta***[4] [magdalena.skrzypiec@umcs.pl]

[1] Institute of Mathematics, Maria Curie-Sklodowska University, Lublin, Poland
[2] Institute of Social and Economic Sciences, Academy of Zamość, Zamość, Poland
[3] Department of Applied Mathematics, Jerusalem College of Technology-Machon Lev, Jerusalem, Israel
[4] Department of Theoretical Chemistry, Maria Curie-Sklodowska University, Lublin, Poland

Let C be an oval (by which we mean a simple closed convex plane curve of class C^2 with positive curvature) and $\alpha \in (0, \pi)$. The set of points at which two support lines of C intersect at angle $\pi - \alpha$ is called an α-isoptic (or simply an isoptic) of C. Isoptics of plane curves are most often considered in the parametric form proposed in [1] and this parametrization seems to be the main tool in the study of isoptics and their generalizations, see for example [2], [5], [6], [7], [8]. Isoptics can be considered also in the nonparametric form, however, implicit equations are known only for a small class of curves, see for example [2],[3].

Our goal is to find orthogonal trajectories of isoptics, but not using the classical approach to this task, which uses implicit equations. We construct parametrizations of orthogonal trajectories to isoptics of ovals, using the solution of a specific Cauchy problem. To prove that the defined function is continuous, we use some version of l'Hôpital's rule for multivariable functions [4]. To illustrate the problem, we analytically determine orthogonal trajectories for a simple example of a circle isoptics, while for more complicated examples we provide and draw numerical solutions, created using the Mathematica program.

In addition to discussing the subject of my research, I'll also share some experiences regarding teaching differential geometry at the University.

Keywords
isoptic curve, support function, evolution, orthogonal trajectory

References

[1] W. CIEŚLAK; A. MIERNOWSKI; W. MOZGAWA, Isoptics of a closed strictly convex curve. *Global differential geometry and global analysis (Berlin, 1990), Lecture Notes in Math.* **1481**, 28–35 (1991).
[2] T. DANA-PICARD; A. NAIMAN; W. MOZGAWA; W. CIEŚLAK, Exploring the isoptics of Fermat curves in the affine plane using DGS and CAS. *Math. Comput. Sci.* **14**(1), 45–67 (2020).

[3] T. DANA-PICARD; N. ZEHAVI; G. MANN, From conic intersections to toric intersections: The case of the isoptic curves of an ellipse. *The Mathematics Enthusiast* **9**(1), 59–76 (2012).
[4] G. R. LAWLOR, l'Hôpitals rule for multivariable functions. *Amer. Math. Monthly* **127**(8), 717–725 (2020).
[5] A. MIERNOWSKI; W. MOZGAWA, On some geometric condition for convexity of isoptics. *Rend. Sem. Mat. Univ. Politec. Torino* **55**(2), 93–98 (1997).
[6] A. MIERNOWSKI; W. MOZGAWA, Isoptics of pairs of nested closed strictly convex curves and Crofton-type formulas. *Beitr. Algebra Geom.* **42**(1), 281–288 (2001).
[7] W. MOZGAWA; M. SKRZYPIEC, Crofton formulas and convexity condition for secantopics. *Bull. Belg. Math. Soc. - Simon Stevin* **16**(3), 435–445 (2009).
[8] D. ROCHERA, On isoptics and isochordal-viewed curves. *Aequat. Math.* **96**(3), 599–620 (2022).

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, July 17-21, 2023
Session on *"Computer Algebra in Education"*

Using CAS in Mathematics Education with the Quadratic Curve Addition Method

Hideyo Makishita[1] [hideyo@shibaura-it.ac.jp]

[1] Department of Civil Engineering, Shibaura Institute of Technology, Tokyo, Japan

The author has proposed a geometric construction that adds the locus of a quadratic curve to a drawing with a ruler and compass. The author calls this method "the quadratic curve addition method." Its characteristic method is based on the fact that the student discerns the foci and directrix, the characteristics of a quadratic curve, from the given conditions. Therefore, the author has made it possible for KeTcindy and LaTeX to generate quadratic curves by telling the dynamic geometry software (Cinderella) the foci and directrix, which are the characteristics of the quadratic curves that they have detected. The circle's center, found by the quadratic curve addition method, is the intersection of those trajectories and figures. The author has shown the effectiveness of this method using Apollonius' problem [1].
In the following, the author presents a case study of the quadratic curve addition method, using the Japanese Sangaku as a subject to show a drawing of a quadratic curve. Concerning the locus of a quadratic curve and CAS, for example, when finding the radius of a circle, it is helpful to express the locus and conditions in terms of equations. In particular, equations representing quadratic curves are generally complex, and the author believes that obtaining solutions by substituting them into CAS, such as Wolfram Alpha, is effective in mathematics education.

The Educational Value of Drawing
Geometric construction is an activity with high educational value. Through such activities, as a result, it is expected to enhance students' problem-solving abilities.
In connection with this study, recent dynamic geometry software has excellent features in GUI plotting and CUI plotting. Therefore, it is possible to transfer mathematical concepts to the software by converting them into scripts, which is expected to provide more opportunities to use mathematics better. If scripting becomes possible, it is conceivable to create a unit vector on the two sides that flank the angle and to construct the angle bisector as the sum of the two vectors. Another possible method is to express one vector of the inner center by the position vectors of the three vertices. The author's mathematical utilization is the teaching method that can be realized by writing mathematics in scrips.

Problem: As shown in Fig.1, place the large circle O so that circles A, B, C, and D are tangent to the interior of the significant process. Let the diameters of the circles O and A be 16 cm, 4.8 cm, respectively. Note that the author quoted Sangaku's problem as an example of a drawing using the quadratic curve addition method.

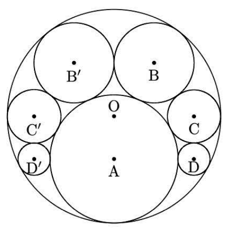


Fig.1

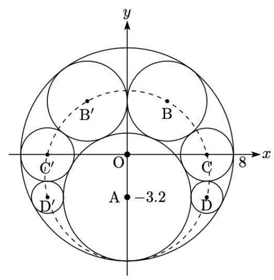


Fig.2

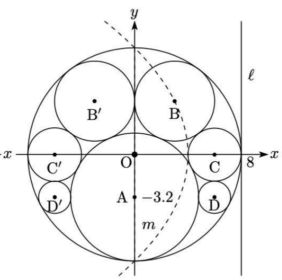


Fig.3

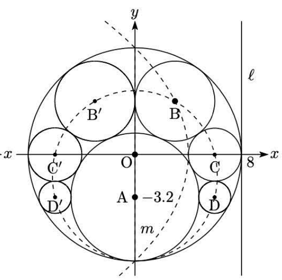


Fig.4

Q1: Find the center of circle B by the quadratic curve addition method.
A1: The center of circle B lies on the locus of an ellipse with point O and point A as foci. However, the sum of the distances from the two points O and A is the sum of the radii of the circles O and A. The center of circle B also lies on the locus of a parabola with O as the focal point and line ℓ as the directrix. □

Q2: Find the radius of the circle B.
A2: In Fig.2, the center of the circle B is on the ellipse.

$$\sqrt{x^2+y^2}+\sqrt{x^2+(y+3.2)^2}=12.8$$

And in Fig.3, the circle's center B lies on the parabola with point O as the focal point and ℓ as the directrix.

$$x=-\frac{1}{16}y^2+4$$

As shown in Fig.4, the point B is the intersection of an ellipse and a parabola.
We solve the system of equations; we obtain $(x, y) = (3, 4), (0, -8)$.
Hence, the center of circle B is $(3, 4)$.
Since $\mathrm{OB} = 5$ cm and the radius of circle O is 8 cm, the radius of circle B is 3 cm. □

The author will present the quadratic curve addition method for some Sangaku problems in this talk. The author will also share the significance and value of the quadratic curve addition method in mathematics education and deepen the discussion with the participants.

Keywords
the quadratic curve addition method, Cinderella, KeTCindy, LaTeX, Wolfram Alpha, Sangaku

Acknowledgment
This work is supported by JSPS KAKENHI Grant Numbers 21K02907.

References

[1] H. MAKISHITA, The problem of Apollonius which was solved by Geometric Construction and Loci of Quadratic Curves. *Transactions of mathematical education for Kosen and University* **25**, 65–86 (2019).

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
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:

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

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. WILOŁAZKA, 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 2023
Warsaw, Poland, | July 17-21, 2023
Session on *"Computer Algebra Modeling in Science and Engineering"*

A discrete SIS model built on the strictly positive scheme

Marcin Choiński[1] [marcin_choinski@sggw.edu.pl]

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

I will present a model which is a discretization of its continuous counterpart. The continuous model was introduced and analyzed in [1]. Both continuous and discrete systems are epidemic models, which are a SIS (*susceptible–infected–susceptible*) type. The models' variables are densities of susceptible (healthy) and infected individuals. As a discretization method, I chose the strictly positive scheme. This scheme preserves positivity of the variables, what is necessary because of their meaning. In my talk I will present the basic properties of the system, including the value of the basic reproduction number $\mathcal{R}_0$ and the existence of stationary states appearing in the system. Further I will discuss local stability of the stationary states. I will also prove the global stability of the state for which there is no infection in the population. Moreover, the behavior of the system for $\mathcal{R}_0 = 1$ will be discussed. In the end of my talk I will justify a lack of a bifurcation in the system. Theoretical results will be complemented with numerical simulations. My results constitute a continuation of the work presented in and [3] and [2].

Keywords
SIS model, local and global stability, discretization

References
[1] M. BODZIOCH; M. CHOIŃSKI; U. FORYŚ, SIS Criss-Cross Model of Tuberculosis in Heterogeneous Population. *Discrete and Continuous Dynamical Systems – Series B* **24**(5), 2169–2188 (2019).
[2] M. CHOIŃSKI; M. BODZIOCH; U. FORYŚ, A Non-standard Discretized SIS Model of Epidemics. *Mathematical Biosciences and Engineering* **19**(1), 115–133 (2022).
[3] 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 2023
Warsaw, Poland, | July 17-21, 2023
Session on *"Computer Algebra Modeling in Science and Engineering"*

On applications of computer algebra systems in queueing theory calculations

Marcin Ziółkowski[1] [marcin_ziolkowski@sggw.edu.pl]

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

In the present talk, the most important aspects of computer algebra systems applications in calculations for classical queueing theory models and their novel modifications are discussed. We present huge computational possibilities of *Mathematica* environment and effective methods of obtaining results connected with main performance characteristics of queueing systems. We investigate solutions of computational problems such as: calculating derivatives of complicated rational functions of many variables with the use of generalized l'Hospital's rule, obtaining exact formulae of Stieltjes convolutions, calculating chosen integral transforms often used in queueing theory and possible applications of generalized density function of random variables and vectors in such computations.

Queueing theory is the field of applied mathematics that has been experiencing great development in recent years. This direction, started in the 20's of the twentieth century by A. K. Erlang, had initially important meaning mainly for telecommunication engineers [2] but its importance was also noticed by scientists from the technical computer science area because it introduced some models that could be used in the process of analyzing or designing of real–life computer systems, e.g. computer networks. The number of publications investigating such models has been still increasing since the moment of a big headway and popularization of computer systems in the 90's of previous century. E.g. in works [4]–[6] authors analyze systems with random volume customers (customers coming to the queueing systems transport information that is written in memory buffer of the system until customer ends his service – see also monograph [3]). The very interesting, novel approach appears also in papers [7–9] that investigate models in which customer's volume is multidimensional. The main problems analyzed for such models are connected with calculating characteristics of the number of customers present in the system, characteristics of the total volume of customers and loss probability. The need of constructing such models is confirmed in projects of some technical devices [10,11].

In the process of mathematical analysis of queueing theory models we face the problem of complicated symbolic computations. The general results often contain functions that are very complex and inconvenient from the numerical point of view as they contain such mathematical concepts like: generating functions, integral transforms or convolutions. Moreover, in obtained formulae we usually find very complicated rational functions of one or many variables what does not let calculate needed numerical characteristics in easy way. For example, we need to calculate derivatives of these functions, often using l'Hospital's rule many times which makes computations are hardly possible without computer algebra systems help. In fact, computer algebra systems give tools to lead complicated symbolic computations successfully. *Mathematica* environment delivers many implemented useful functions letting calculate integral transforms and their inversions or derivatives of complicated rational functions [1]. The big advantage of computer algebra systems is also storing previous results in memory and the possibility to use them again in next steps of computations despite of their complexity. These facts confirm that computer algebra systems are fantastic tool being helpful in the process of queueing models analyzing.

Keywords
Queueing models, Queueing systems with random volume customers and sectorized memory buffer, Generalized l'Hospital's rule, Stieltjes convolution, Laplace – Stieltjes transform

References

[1] M. L. ABELL; J. P. BRASELTON, *The Mathematica Handbook*, Elsevier, 1992.
[2] P. P. BOCHAROV; C. D'APICE; A. V. PECHINKIN; S. SALERNO, *Queueing Theory*, VSP, Utrecht-Boston, 2004.
[3] O. TIKHONENKO, *Computer Systems Probability Analysis*, Akademicka Oficyna Wydawnicza EXIT, Warsaw, 2006 (In Polish).
[4] V. NAUMOV; K. SAMUILOV; A. SAMUILOV, On the total amount of resources occupied by serviced customers. *Automation and Remote Control* **77**, 1419–1427 (2016).
[5] K. KEROBYAN; R. COVINGTON; R. KEROBYAN; K. ENAKOUTSA, An infinite–server queueing $MMAP_k/G_k/\infty$ model in semi–Markov random environment subject to catastrophes. In *Communications in Computer and Information Science*, Dudin A. et al. (eds), 195–212, Springer, Cham, 2018.
[6] E. LISOVSKAYA; S. MOISEEVA; M.PAGANO, Multiclass $GI/GI/\infty$ queueing systems with random resource requirements. In: *Communications in Computer and Information Science*, Dudin A. et al. (eds), 129–142, Springer, Cham, 2018.
[7] O. TIKHONENKO; M.ZIÓŁKOWSKI; M. KURKOWSKI, $M/G/n/(0,V)$ Erlang queueing system with non–homogeneous customers, non–identical servers and limited memory space. *Bulletin of the Polish Academy of Sciences: Technical Sciences* **67**(3), 489–500 (2019).
[8] O. TIKHONENKO; M. ZIÓŁKOWSKI; W. M. KEMPA, Queueing systems with random volume customers and a sectorized unlimited memory buffer. *International Journal of Applied Mathematics and Computer Science* **31**(3), 471–486 (2021).
[9] M. ZIÓŁKOWSKI; O. TIKHONENKO, Single–server queueing system with limited queue, random volume customers and unlimited sectorized memory buffer. *Bulletin of the Polish Academy of Sciences: Technical Sciences* **70**(6), article id. e143647 (2022).
[10] H.-K. KIM, System and method for processing multimedia packets for a network, *Technical report, US Patent No. 7,236,481 B2*, `patents.google.com/patent/US7236481B2/en` (2002).
[11] X. CHEN; A. STIDWELL; M. HARRIS, Radiotelecommunications apparatus and method for communications internet data packets containing different types of data, *Technical report, US Patent No. 7,558,240 B2*, `patents.google.com/patent/US7558240B2/en` (2009).

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session on *“Computer Algebra Modeling in Science and Engineering”*

Analyzing electric circuits with Computer Algebra

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

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

This report shows how starting from classic electric circuits embodying common electric components we have reached semi-complicated circuits embodying the same components that analyzing the signal characteristics requires a Computer Algebra System. Our approach distinguishes itself from the electrical engineers' (EE) approach which relies on utilizing commercially available software. Our approach step-by-step shows how Kirchhoff's rules are applied conducive to the needed circuit information. It is shown for the case at hand the characteristic information is a set of coupled differential equations and that with the help of *Mathematica* numeric solutions are sought. Our report paves the research road for unlimited creative similar circuits with any degree of complications. Occasionally, by tweaking the circuits we have addressed the “what if” scenarios widening the scope of the investigation. Justification of the accuracy of our analysis for the generalized circuits is cross-checked by arranging the components symmetrizing the circuit leading to an intuitively predictable reasonable result. *Mathematica* codes are embedded assisting the interested reader in producing and extending our results.

Keywords
Characteristics of Electric Circuits, DC and AC Driven Circuits, Computer Algebra System, *Mathematica*

Applications of Computer Algebra – ACA 2023
July 17-21, 2023
Session on *"Computer Algebra Modeling in Science and Engineering"*

LMS with simple modeling developed by extended CindyJS and Maxima

Setsuo Takato[1], ***Hideyo Makishita***[2] [takato@jcom.home.ne.jp]

[1] KeTCindy Center, Magnolia Inc., Kisarazu, Japan
[2] Department of Civil Engineering, College of Engineering, Shibaura Institute of Technology, Tokyo, Japan

KeTLMS(KeTCindy Learning Management System) is a system to distribute mathematical questions, collect answers and score them using some platform such as Google Classroom, Teams or Moodle for actual communication. The point is the content consists of only one line of text described according to KeTMath rule, simple one-dimensional formula description rule which we have defined. For example, the question

Differentiate [1] $y = \dfrac{x^2+4x+3}{\sqrt{x}}$ [2] $y = t^3 \cos 2t$

is described with LaTeX as

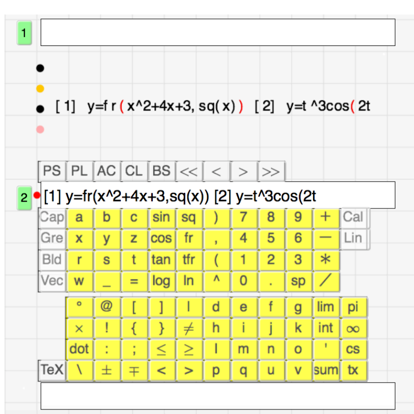
```
Differentiate
[1] $y=\dfrac{x^2+4x+3}{\sqrt{x}}$ [2] $y=t^3\cos 2t$.
```

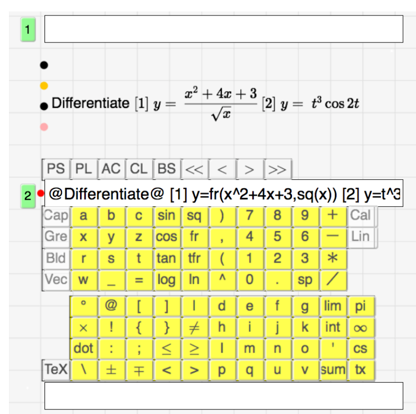
On the other hand, our notatation would be

```
@Differentiate@ [1] y=fr(x^2+4x+3,sq(x)) [2] y=t^3cos(2t).
```

Remark) @expression@ means the expression is not a mathematical formula.

One-dimentional expression is suitable for sending and receiving, but not for reading. So we developed an HTML application KeTMath with our software KeTCindyJS, which is the cooperation of KeTpic we have been developing, dynamic geometry software Cinderella and CindyJS which is a framework almost compatible with Cinderella.



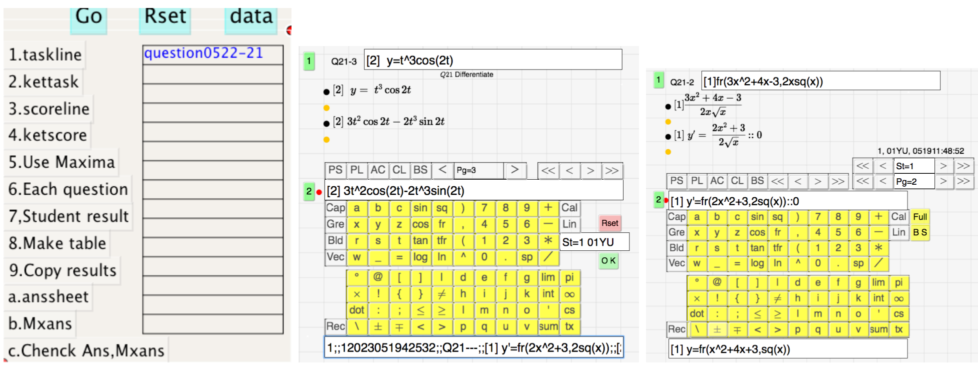


KeTLMS is essentially based on this method. The procedure is as follows.

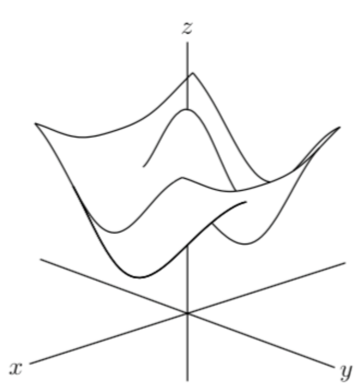
1. Make a question file according to KeTMath rule.

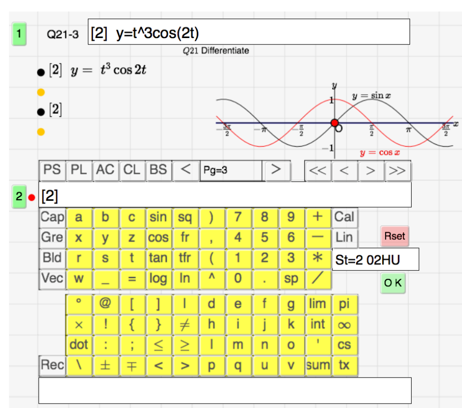
```
Q
@Differentiate@
[1] y=fr(x^2+4x+3,sq(x))
[2] y=t^3cos(2t)
Ans
[1] fr(3x^2+4x-3,2xsq(x))
[2] 3t^2cos(2t)-2t^3sin(2t)
```

2. Create kettask.html using 'toolketmath.cdy', and distribute it to students.
3. Collect answers, and create ketscore.html to score them.
4. Maxima can be useful for simple questions. KeTLMS has a function to use it.



One can insert figures to the kettask.html. For three dimentional figures, Ketcindy call gcc from the inside to speed up hiddlen line removal which is important to create figures of 3d surfaces. Not only static figures, one can also embed interactive ones. Embedding interactive HTML of three dimentional figures will be future work.





Keywords
LaTeX, Maxima, KeTCindy

References

[1] S. TAKATO; A. MCANDREW; J.A. VALLEJO; M. KANEKO,Collaborative use of KeTCindy and free Computer Algebra Systems. *Mathematics in Computer Science* **11**, 503–514 (2017).

Applications of Computer Algebra – ACA 2023
July 17-21, 2023
Session on *“Computer Algebra Modeling in Science and Engineering”*

Billiards: At the intersection of Math, Physics and Computer Algebra

***Setsuo Takato*[1], *José A Vallejo*[2]** [jvallejo@mat.uned.es]

[1] KeTCindy Center, Magnolia Inc., Kisarazu, Japan
[2] Departamento de Matemáticas Fundamentales, Universidad Nacional de Educación a Distancia, Madrid, Spain

Billiards, interpreted as dynamical systems, have a lot of interesting geometric properties [2], [3]. Particularly, the dynamics on a billiard whose boundary is a conic serves as an excellent visualization aid for some deep results in affine and projective geometry. In this talk we will be interested in the case of elliptic billiards. From the point of view of Physics, they are quite manageable, being integrable systems, yet they show phenomena such as the appearance of caustics, closed orbits of any prescribed period [1], and the like. The fact that they are geometrically describable makes them suitable to be analyzed with a Computer Algebra System (CAS), and we will illustrate how to model their main features using Maxima and KeTCindy, in such a way that they can be introduced in math, physics and engineering courses (but also as a tool in research tasks).

Keywords
KeTCindy, Maxima, Billiards, Dynamical Systems

References

[1] M. SIEBER, *Semiclassical transition from an elliptical to an oval billiard* J. Phys. A: Math. Gen. **30** 13 (1997) 4563.
[2] U. A. ROZIKOV, *An introduction to mathematical billiards*. World Scientific Publishing, Singapore, 2019.
[3] S. TABACHNIKOV, *Geometry and billiards*. American Mathematical Society, Providence (RI), 2005.

Applications of Computer Algebra – ACA 2023
July 17-21, 2023
Session on *"Computer Algebra Modeling in Science and Engineering"*

Computation of normal forms for systems with many parameters

Tatjana Petek[1,4] ***and Valery G. Romanovski***[1,2,3] `[valerij.romanovskij@um.si]`

[1] Faculty of Electrical Engineering and Computer Science, University of Maribor, Maribor, Slovenia
[2] Faculty of Natural Science and Mathematics, University of Maribor, Maribor, Slovenia
[3] Center for Applied Mathematics and Theoretical Physics, University of Maribor, Maribor, Slovenia
[4] Institute of Mathematics, Physics and Mechanics, Ljubljana, Slovenia

There are two ways to compute Poincaré-Dulac normal forms of systems of ODEs. Under the original approach used by Poincaré the normalizing transformation is explicitly computed. On each step, the normalizing procedure requires the substitution of a polynomial to a series. Under the other approach, a normal form is computed using Lie transformations. In this case, the changes of coordinates are performed as actions of certain infinitesimal generators. In both cases, on each step the homological equation is solved in the vector space of polynomial vector fields V_j^n where each component of the vector field is a homogeneous polynomial of degree j. We present the third way of computing normal forms of polynomial systems of ODEs where the coefficients of all terms are parameters. Although we use Lie transforms the homological equation is solved not in V_j^n but in the vector space of polynomial vector fields where each component is a homogeneous polynomial in the parameters of the system. It is shown that the space of the parameters is a kind of dual space and the computation of normal forms can be performed in the space of parameters treated as the space of generalized vector fields. The approach provides a simple way to parallelize the normal form computations opening the way to compute normal forms up to higher order than under previously known two approaches.

Keywords
Poincaré-Dulac Normal Form, Lie Transform, Lie Algebra of Vector Fields

References

[1] T. PETEK AND V. G. ROMANOVSKI, Computation of Normal Forms for Systems with Many Parameters, arXiv:2305.01739, 2023.

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session on *"Computer Algebra Modeling in Science and Engineering"*

Spin 1 particle with anomalous magnetic moment in external uniform electric field, solutions with cylindric symmetry

***Alina Ivashkevich*[1], *Victor Red'kov*[1], *Alexander Chichurin*[2]** [achichurin@kul.pl]

[1] Department of Fundamental Interactions and Astrophysics, B.I. Stepanov Institute of Physics, Minsk, Belarus
[2] Department of Mathematical Modeling, The John Paul II Catholic University of Lublin, Lublin, Poland

The study of a spin 1 particle has a long history – for example see [1]-[4]. In the present paper we will adhere the the general technics developed in [5], [6]. A generalized 10-dimensional Duffin – Kemmer equation [7] for spin 1 particle with anomalous magnetic moment is examined in cylindric coordinates (t, r, ϕ, z) in presence of external uniform electric field oriented along the axis z. On solutions, we diagonalize operators of the energy and third projection of the total angular momentum. First we derive the system of 10 equations in partial derivatives for functions $F_i(r, z) = G_i(r)H_i(z)$ $(i = \overline{1, 10})$. The use of the method based on projective operators permits us to express 10 variables $G_i(r)$ through only 3 different functions $f_1(r), f_2(r), f_3(r)$, which are solved in Bessel functions. After that we derive the system of 10 first order differential equations for functions $H_i(z)$. This system reduces to one independent equation for a separate function and to the system of two linked equations for two remaining primary functions. The last system after diaginalization of the mixing matrix gives two separated equations for new variables. All three equations for basic functions are solved in terms of the confluent hypergeometric functions. Thus, the complete system of solutions for the vector particle with anomalous magnetic moment in presence of external electric field is found.

Keywords
spin 1 particle, anomalous magnetic moment, external electric field, cylindrical symmetry, method of the projective operators, partial differential equations, exact solutions

References

[1] A. PROCA, Sur les equations fondamentales des particules élémentaires. *C. R. Acad. Sci. Paris*, **202**, pp. 1490–1492 (1936).
[2] R.Y. DUFFIN, On the characteristic matrices of covariant systems. *Phys. Rev.*, **54 (12)**, pp. 1114–1114 (1938).
[3] E. SCHRÖDINGER, Pentads, tetrads, and triads of meson matrices. *Proc. Roy. Irish. Acad. A.*, **48**, pp. 135–146, (1943).

[4] N. KEMMER, On the theory of particles of spin 1. *Helv. Phys. Acta.*, **33 (8)**, pp. 829–838 (1960).
[5] E.M. OVSIYUK; V.V. KISEL; V.M. RED'KOV, *Maxwell Electrodynamics and Boson Fields in Spaces of Constant Curvature*, Nova Science Publishers Inc., New York, 2014.
[6] V.V. KISEL; E.M. OVSIYUK; O.V. VEKO; Y.A. VOYNOVA; V. BALAN;, V.M. RED'KOV, *Elementary Particles with Internal Structure in External Fields, Vol. I, II*, Nova Science Publishers Inc., New York, 2018.
[7] A. SHAMALY; A.Z. CAPRI,Unified theories for massive spin 1 fields. *Can. J. Phys.*, **51**, pp. 1467–1470 (1973).

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17 – 21, 2023
Session on *"Computer Algebra Modeling in Science and Engineering"*

On stability of stationary motion of the 3D swinging Atwood machine

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]). The mass m_1 is allowed to swing in two dimensions and its behaves like a spherical pendulum of variable length while the mass m_2 is constrained to move only along a vertical. Such a system has three degrees of freedom and its equations of motion may be written in the form

$$\begin{aligned} r\ddot{\theta} &= -g\sin\theta - 2\dot{r}\dot{\theta} + \frac{p_\varphi^2\cos\theta}{r^3\sin^3\theta}, \\ r^2\sin^2\theta\dot{\varphi} &= p_\varphi = const, \\ (2+\varepsilon)\ddot{r} &= r\dot{\theta}^2 - g(1+\varepsilon-\cos\theta) + \frac{p_\varphi^2}{r^3\sin^2\theta}. \end{aligned} \tag{1}$$

Here the dot above the symbol denotes a total time derivative of the corresponding function, the variables r, θ, φ describe geometrical configuration of the system, g is a gravity constant, $\varepsilon = (m_2 - m_1)/m_1$, and p_φ is an itergal of motion determined from the initial conditions. In the case of $p_\varphi = 0$ the mass m_1 oscillates on a vertical plane and we obtain the swinging Atwood machine which may demonstrate a periodic motion (see [2, 3]).

One can easily check that there exists an exact particular solution to equations (1) of the form

$$\varphi(t) = \sqrt{\frac{g(1+\varepsilon)}{r_0}}t + \varphi_0,\ r(t) = r_0,\ \theta(t) = \theta_0 = \arccos(1/(1+\varepsilon)). \tag{2}$$

Solution (2) describes a uniform motion of body m_1 in a horizontal plane on a circular orbit of radius $r_0\sin\theta_0$. Simulation of the system motion shows that small variation of the initial conditions results only in small perturbation of the body m_1 orbit. Analyzing the Hamiltonian function of the system and applying the stability theory, we have proved that solution (2) is stable with respect to the variables $r, \dot{r}, \theta, \dot{\theta}, \dot{\varphi}$.

Keywords
3D Swinging Atwood machine, equations of motion, stationary solution, stability

References

[1] A.N. PROKOPENYA, Motion of a swinging Atwood's machine: simulation and analysis with Mathematica. *Mathematics in Computer Science* **11**(3-4), 417–425 (2017).
[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, Stability analysis of periodic motion of the swinging Atwood machine. In: Boulier, F., England, M., Sadykov, T.M., Vorozhtsov, E.V. (eds.), Computer Algebra in Scientific Computing. CASC 2022. LNCS 13366. Springer, Cham (2022), p. 288–299.

Applications of Computer Algebra – ACA 2023
Warsaw. Poland | July 17-21, 2023
Session on *"Computer Algebra Modeling in Science and Engineering"*

Semi-algebraic representations for the multistationarity region of reaction networks

AmirHosein Sadeghimanesh[1]***, Matthew England***[1]
[amirhossein.sadeghimanesh@coventry.ac.uk]

[1] Centre for Computational Sciences and Mathematical Modelling, Coventry University, Coventry, UK

The behavior of a chemical reaction network equipped with mass-action kinetics can be modelled by a polynomial ODE system. The equilibriums of this ODE system are the solutions to a system of polynomial equations. The model usually does not only involve variables, concentrations of the substances, but also some parameters such as reaction rates and constants of conservation laws. An important question is whether there exists a choice of parameter values for which the system has more than one equilibrium: in that case we say the network can exhibit multistationary behavior. The next important question is to describe the parameter region where the network is multistationary. In this talk we compare several approaches to describe the multistationarity region. In theory tools such as Cylindrical Algebraic Decomposition can provide an exact semi-algebraic description of this region. However, in practice due to its worst case doubly exponential complexity it is usually infeasible for a normal computer. Sacrificing the exactness in exchange with lower complexity, one still can get a semi-algebraic description of the multistationarity region using a sampling or a rectangular representation of the region and polynomial superlevel sets.

Keywords
Polynomial superlevel set, Multistationarity, Parameter analysis

References

[1] A. Sadeghimanesh and M. England, Polynomial superlevel set representation of the multistationarity region of chemical reaction networks. *BMC Bioinformatics* **23**, article number 391 (2022).
[2] R. Bradford, J. H. Davenport, M. England, H. Errami, V. Gerdt, D. Grigoriev, C. Hoyt, M. Košta, O. Radulescu, T. Sturm, A. Weber, Identifying the parametric occurrence of multiple steady states for some biological networks. *Journal of Symbolic Computation* **98**, 84-119 (2020).
[3] E. Feliu and A. Sadeghimanesh, Kac-Rice formulas and the number of solutions of parametrized systems of polynomial equations. *Mathematics of Computation* **91**, 2739-2769 (2022).

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17 – 21, 2023
Session on *“Computer Algebra Modeling in Science and Engineering”*

Derivation of the evolution equations in the restricted three-body problem with variable masses by using Computer Algebra

Alexander Prokopenya[1], ***Mukhtar Minglibayev***[2,3]
Aigerim Ibraimova[2,3] [ibraimova@aphi.kz]

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

Observational astronomy states that celestial bodies are unsteady, their masses, sizes, shapes and structures change in the process of evolution. Variability in the masses of celestial bodies, especially at the nonstationary stage of the system, significantly affects the further dynamical evolution of this system as a whole [1, 2, 3]. In this connection, we consider the restricted three-body problem with variable mass in the presence of reactive forces. The problem was investigated by methods of perturbation theory, based on the aperiodic motion along a quasi-conic section developed by us [4]. The system of differential equations of perturbed motion in oscillating variables of aperiodic motion along a quasi-conic section in the form of Newton's equation was derived [5]. By using Computer Algebra we obtained the equations of secular perturbation of the restricted three-body problem with variable masses in the presence of reactive forces [6].

Acknowledgments
This research is funded partially by the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grants No. AP14869472).

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] 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).
[3] EGGLETON P. *Evolutionary processes in binary and multiple stars*. Cambridge University Press. – 2006. – P.332.

[4] M. MINGLIBAYEV, *Dynamics of gravitating bodies with variable masses and sizes*. LAMBERT Academic Publishing, Saarbrücken, 2012.
[5] M. MINGLIBAYEV; CH. OMAROV; A. IBRAIMOVA, New forms of the perturbed motion equation. *RNAS RK*. **2**(330), 5–13 (2020).
[6] IBRAIMOVA A.T., MINGLIBAYEV M.ZH., PROKOPENYA A.N. Study of Secular Perturbations in the Restricted Three-Body Problem of Variable Masses Using Computer Algebra // Computational Mathematics and Mathematical Physics. **63**(1), 115–125 (2023).

Applications of Computer Algebra – ACA'2023
Warsaw, Poland | July 17 – 21, 2023
Session on *"Computer Algebra Modeling in Science and Engineering"*

The problem of many bodies with isotropically varying masses

Mukhtar Minglibayev[1,2]***, Alexander Prokopenya***[3]
Aiken Kosherbayeva[1] [kosherbaevaayken@gmail.com]

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

The number of confirmed exoplanetary systems is more than 4000 to date [1] and it is growing up every day. The parent star and exoplanets are non-stationary [2]. It means that the investigation of a multi-planetary system with variable masses is actual in celestial mechanics and astronomy. Due to the non-stationarity of celestial bodies, the mathematical model of their motion becomes more complicated.

In the present talk, we investigate the dynamic evolution of the system of many bodies with isotropically varying masses. We apply the method of canonical perturbation theory developed for solutions of such non-stationary problems in [3]. Doing quite cumbersome symbolic calculations with the computer algebra system Wolfram Mathematica [4], we calculated the perturbing function in the form of power series in small parameters (analogues of eccentricities and inclinations). Averaging the perturbing function over the mean longitudes and computing its derivatives with respect to the canonical variables, we derived the evolution equations describing the secular perturbations of the orbital elements in analytical form [5]. As an example, we have considered the K2-3 exoplanetary system (see [6]) and obtained numerical solutions of the evolution equations.

Keywords: four body problem, variable mass, dynamic evolution, secular perturbations

Acknowledgments
This research is funded by the Committee of Science of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No. AP14869472)

References

[1] EXOPLANET EXPLORATION, *url:https://exoplanets.nasa.gov/*. Last update: May 11, 2023.
[2] T.B. OMAROV, Non-Stationary Dynamical Problems in Astronomy. *New-York: Nova Science Publ.Inc. P.260. ISBN:1-59033-331-4*, (2002).

[3] M. Zh. Minglibayev, *Dinamika gravitiruyushchikh tel s peremennymi massami i razmerami [Dynamics of gravitating bodies with variable masses and sizes].* LAP LAMBERT Academic Publishing. P.224. Germany.ISBN:978-3-659-29945-2 (in Russ.).
[4] A. N. Prokopenya, Reshenie fizicheskih zadach s ispol'zovaniem sistemy Mathematica [Solving physical problems using the Mathematica system]. *BSTU Publishing, Brest., P.260. ISBN 985-493-024-6*, (2005). (in Russ.).
[5] A. N. Prokopenya, M. Zh. Minglibayev, A. B. Kosherbaeva, Derivation of Evolutionary Equations in the Many-Body Problem with Isotropically Varying Masses Using Computer Algebra. *Programming and Computer Software.* **48**(2), P. 107–115, (2022) DOI:10.1134/S0361768822020098.
[6] Almenara et al., A HARPS view on K2-3. *Astronomy & Astrophysics*, **581**(L7), 6 pp. DOI: 10.1051/0004-6361/201525918, (2015).

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17 – 21, 2023
Session on *"Computer Algebra Modeling in Science and Engineering"*

Investigation of a two-planetary problem of three bodies with variable masses varying anisotropically at different rates

***Mukhtar Minglibayev*[1,2], *Alexander Prokopenya*[3],**
***Zhanar Imanova*[1]** [Imanovazhanar0884@gmail.com]

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

Masses of real celestial bodies may vary anisotropically [1, 2]. Due to the anisotropic change of the masses reactive forces appear and this complicates the problem significantly. We investigated a two-planetary problem of three bodies with variable masses in the presence of reactive forces and obtained the equations of perturbed motion in the framework of Newton's formalism [3]. The equations of motion in the orbital coordinate system, in contrast to the Lagrange equations [4], are convenient for taking into account reactive forces. The expansion of perturbing functions is a time-consuming analytical calculation and leads to very cumbersome analytical expressions. In the problem under consideration, we calculated the power expansions of the perturbing functions in terms of small parameters up to the second order inclusive. In the non-resonant case, we obtained the evolutionary equations determining the secular perturbations of the orbital elements. All symbolic calculations were performed with the computer algebra system Wolfram Mathematica [5].

Keywords: two-planetary three-body problem, variable mass, evolutionary equations, Wolfram Mathematica.

Acknowledgments
This research is funded by the Committee of Science of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No. AP14970491)

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] A. N. PROKOPENYA, Solving Physics Problems Using Mathematica. BSTU Press, Brest, 2005.

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session *"D-Finite Functions and Beyond: Algorithms, Combinatorics, and Arithmetic"*

Reduction based creative telescoping for definite summation of P-recursive sequences: the Integral Basis Approach

***Shaoshi Chen*[1,2], *Lixin Du*[3], *Manuel Kauers*[3]** [lixin.du@jku.at]

[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

Integral bases have been used for designing reduction-based telescoping algorithm for algebraic functions [1] and D-finite functions [2]. The notion of integral bases for D-finite functions has recently been generalized to P-recursive sequences [3]. As a discrete analogue, we develop a reduction-based creative telescoping algorithm for P-recursive sequences via integral bases.

Keywords
Creative telescoping, Holonomic sequences, Symbolic summation

References
[1] SHAOSHI CHEN; MANUEL KAUERS; CHRISTOPH KOUTSCHAN, *Reduction-Based Creative Telescoping for Algebraic Functions*. In Proceedings of the 2016 International Symposium on Symbolic and Algebraic Computation (ISSAC' 16), pages 175–182, New York, NY, 2016.
[2] SHAOSHI CHEN; LIXIN DU; MANUEL KAUERS, *Hermite Reduction for D-finite Functions via Integral Bases*. In Proceedings of the 2023 International Symposium on Symbolic and Algebraic Computation (ISSAC' 23), New York, NY, 2023.
[3] SHAOSHI CHENA; LIXIN DU; MANUEL KAUERS; THIBAUT VERRON, *Integral Bases for P-Recursive Sequences*. In Proceedings of the 2020 International Symposium on Symbolic and Algebraic Computation (ISSAC' 20), pages 91–98. New York, NY, 2020.

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session *"D-Finite Functions and Beyond: Algorithms, Combinatorics, and Arithmetic"*

Automatic Lucas-type congruences

Armin Straub[1] [straub@southalabama.edu]

[1] Department of Mathematics & Statistics, University of South Alabama, Mobile, USA

Rowland and Zeilberger [3] devised an approach to algorithmically determine the modulo p^r reductions of values of combinatorial sequences representable as constant terms (building on work of Rowland and Yassawi [4]). The resulting p-schemes are systems of recurrences and, depending on their shape, are classified as automatic or linear. We review this approach and suggest, as in [5], a third natural type of scheme that combines benefits of automatic and linear ones. As an example of the utility of these "scaling" schemes, we confirm and extend a conjecture of Rowland and Yassawi [4] on Motzkin numbers.

It is a well-known and beautiful classical result of Lucas that, modulo a prime p, the binomial coefficients satisfy the congruences

$$\binom{n}{k} \equiv \binom{n_0}{k_0}\binom{n_1}{k_1}\cdots\binom{n_r}{k_r},$$

where n_i, respectively k_i, are the p-adic digits of n and k. Many interesting integer sequences have been shown to satisfy versions of these congruences. For instance, Gessel [1] has done so for the numbers used by Apéry in his proof of the irrationality of $\zeta(3)$. We make the observation that a sequence satisfies Lucas congruences modulo p if and only if its values modulo p can be described by a linear (or scaling) p-scheme with a single state. This simple observation suggests natural generalizations of the notion of Lucas congruences. To illustrate this point, we derive explicit generalized Lucas congruences for integer sequences that can be represented as certain constant terms. This part of the talk is based on joint work [2] with Joel Henningsen.

Keywords
Lucas congruences, constant terms, diagonals, finite-state automata, linear p-schemes, binomial sums, Apéry-like numbers, Catalan numbers, Motzkin numbers

References

[1] I. GESSEL, Some congruences for Apéry numbers. *Journal of Number Theory* **14**(3), 362–368 (1982).
[2] J. HENNINGSEN; A. STRAUB, Generalized Lucas congruences and linear p-schemes. *Advances in Applied Mathematics* **141**, 1–20, #102409 (2022).
[3] E. ROWLAND; D. ZEILBERGER, A case study in meta-automation: automatic generation

of congruence automata for combinatorial sequences. *Journal of Difference Equations and Applications* **20**(7), 973–988 (2014).
[4] E. ROWLAND; R. YASSAWI, Automatic congruences for diagonals of rational functions. *Journal de Théorie des Nombres de Bordeaux* **27**(1), 245–288 (2015).
[5] A. STRAUB, On congruence schemes for constant terms and their applications. *Research in Number Theory* **8**(3), 1–21, #42 (2022).

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session *"D-Finite Functions and Beyond: Algorithms, Combinatorics, and Arithmetic"*

Linear recurrence sequences in the OEIS

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

[1] Institute for Algebra, Johannes Kepler University Linz, Austria

As of spring 2023, the On-Line Encyclopedia of Integer Sequences (OEIS) contains about 360 000 sequences [1]. Referencing an invited talk by Bruno Salvy at ISSAC 2005 [2], it is frequently stated that around 25% of the sequences in the OEIS satisfy a linear recurrence with polynomial coefficients. Using different guessing techniques we try to verify this claim and additionally give an estimate for the number of sequences satisfying a linear recurrence with constant coefficients. Furthermore, we study how this ratio changed over the past two decades and investigate the orders and degrees (in the case of polynomial coefficients) of the guessed recurrences.

Automatically proving positivity of a sequence which satisfies a linear recurrence is, in general, a difficult task [3]. Several algorithms are known which can be used to prove positivity for certain classes of these sequences where the recurrences have only constant coefficients. We take some of the sequences from the OEIS as a test set to examine how powerful these algorithms are [4].

Keywords
Recurrences, Guessing, OEIS, Positivity

References

[1] OEIS Foundation Inc., *The On-Line Encyclopedia of Integer Sequences*. Published electronically at `http://oeis.org`, 2023
[2] Bruno Salvy, D-finiteness: algorithms and applications. In *ISSAC '05: Proceedings of the 2005 international symposium on Symbolic and algebraic computation*, 2005.
[3] Joël Ouaknine, James Worrell, Positivity problems for low-order linear recurrence sequences. In *SODA'14: Proceedings of the twenty-fifth annual ACM-SIAM symposium on Discrete algorithms*, 2014.
[4] Philipp Nuspl, Veronika Pillwein, A Comparison of Algorithms for Proving Positivity of Linearly Recurrent Sequences. *Computer Algebra in Scientific Computing*, volume 13366 of *LNCS*. 2022.

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session *"D-Finite Functions and Beyond: Algorithms, Combinatorics, and Arithmetic"*

Reduction based creative telescoping for definite summation of D-finite functions: the Lagrange Identity Approach

Hadrien Brochet[1,2]***, Bruno Salvy***[2] [hadrien.brochet@inria.fr]

[1] Inria, Palaiseau, France
[2] Inria, ENS de Lyon, Lyon, France

Creative telescoping is an algorithmic method initiated by Zeilberger [1] to compute definite sums and integrals. In the context of summation with regard to the variable t, given a summand $F(t, x_1, \ldots, x_m)$, where each x_i is a variable with an associated linear operator ∂_i (generally, differentiation or shift or q-shift operator), the goal is to construct identities of the form

$$\sum_{\boldsymbol{\alpha}} c_{\boldsymbol{\alpha}}(x_1, \ldots, x_m)\boldsymbol{\partial}^{\boldsymbol{\alpha}}(F) = G(t+1, x_1, \ldots, x_m) - G(t, x_1, \ldots, x_m), \tag{1}$$

where the sum is over a finite number of multi-indices $\boldsymbol{\alpha}$ and we use the multi-exponent notation $\boldsymbol{\partial}^{\boldsymbol{\alpha}} = \partial_1^{\alpha_1} \cdots \partial_m^{\alpha_m}$. Such an identity can in many applications be summed over t. Its right-hand side telescopes by design. Since the coefficients $c_{\boldsymbol{\alpha}}$ do not depend on the variable t, the left-hand side results in an operator applied to the definite sum of F. From there, other algorithms can be applied to compute information on the sum. The left-hand side of (1) is called a *telescoper* of F and the function G in the right-hand side is the corresponding *certificate*. Over the years, efficiency issues have led to the development of creative telescoping algorithms based on reductions. They avoid the computation of potentially large certificates and they compute telescopers in a more incremental fashion. In 2018 Bostan-Chyzak-Lairez-Salvy [2] published a reduction based algorithm for computing integrals of arbitrary D-finite functions. It was adapted to the summation case by van der Hoeven [4].

In my talk I will describe a new reduction based creative telescoping algorithm that is an adaption of the two previous ones. It computes telescopers for definite sums of D-finite functions as well as the associated certificates in a compact form. The algorithm relies on a discrete analogue of the generalized Hermite reduction introduced in [2] or equivalently, a generalization of the Abramov-Petkovšek reduction [3]. In contrast to van der Hoeven's algorithm, ours always returns the minimal order telescopers.

Keywords
Creative Telescoping, Symbolic Summation, D-finite Functions, Lagrange Identity, Hermite Reduction

References

[1] D. ZEILBEGER, A fast algorithm for proving terminating hypergeometric identities. *Discrete Mathematics* 80(2), 207–211, 1990.

[2] A.BOSTAN, F. CHYZAK, P. LAIREZ, B. SALVY, Generalized hermite reduction, creative telescoping and definite integration of D-finite functions, In *Proceedings of the International Symposium on Symbolic and Algebraic Computation*, 2018.

[3] A. ABRAMOV, M.PETKOVŠEK, Minimal decomposition of hypergeometric terms, In *Proceedings of the International Symposium on Symbolic and Algebraic Computation*, 2001.

[4] J. VAN DER HOEVEN, Creative telescoping using reductions. *preprint*, 2018.

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session *"D-Finite Functions and Beyond: Algorithms, Combinatorics, and Arithmetic"*

How a linear recurrence problem inspired a solution in algebraic geometry

Catherine St-Pierre[1,2] [catherine.st-pierre@uwaterloo.ca]

[1] Cheriton School of Computer Science, University of Waterloo Waterloo, Ontario, Canada
[2] University Paris-Saclay, Palaiseau, France

We review existing techniques to find terms in linearly recurrent sequences, such as Fiduccia's algorithm [1], and we focus on what can be done in some specific cases, such as when the recurrence is not square-free [2]. We rediscuss a map inspired by van der Hoeven and Lecerf [3] and how it ended up inspiring a method we use to address different problems arising from algebraic geometry or algebra, *e.g.* finding high powers of matrices [4]. We present some of the general lines of one of our recent works in the context of bivariate Gröbner bases [5], which is tailored to address the question of the local structure of the intersection of plane curves. In particular, we discuss the interest in moving the primary component to the origin and how it arises from a similar approach to what we use for sequences.

Keywords
Linear recurrence, algebraic geometry

References

[1] C. M. FIDUCCIA, An efficient formula for linear recurrences. *SIAM Journal on Computing*, 14(1), 106–112 (1985).
[2] S. G. HYUN; S. MELCZER; É. SCHOST; C. ST-PIERRE, Change of basis for m-primary ideals in one and two variables. In *Proceedings of the 2019 on International Symposium on Symbolic and Algebraic Computation*, 227–234 (2019).
[3] J. VAN DER HOEVEN; G. LECERF, Composition modulo powers of polynomials. In *Proceedings of the 2017 ACM on International Symposium on Symbolic and Algebraic Computation*, 445–452 (2017).
[4] M. GIESBRECHT, Nearly optimal algorithms for canonical matrix forms. *SIAM Journal on Computing*, 24(5), 948–969 (1995).
[5] É. SCHOST; C. ST-PIERRE, Newton iteration for lexicographic Gröbner bases in two variables. Preprint arXiv:2302.03766 (2023).

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session *"D-Finite Functions and Beyond: Algorithms, Combinatorics, and Arithmetic"*

Two applications of the telescoping method

***Qing-Hu Hou*[1], Guo-Jie Li[2], Na Li[1], Ke Liu[3]** [qh_hou@tju.edu.cn]

[1] School of Mathematics, Tianjin University, Tianjin, China
[2] School of Science, Hainan University, Hainan, China
[3] College of Science, Chongqing University of Technology, Chongqing, China

In this talk, we will give two applications of telescoping method.

The first one focuses on series involving π. In [5], Sun derived several identities involving π by telescoping method. For example, from Bauer's series [1]

$$\sum_{k=0}^{\infty}(4k+1)\frac{\binom{2k}{k}^3}{(-64)^k}=\frac{2}{\pi}$$

and the telescoping sum

$$\sum_{k=0}^{n}\frac{(16k^3-4k^2-2k+1)\binom{2k}{k}^2}{(2k-1)^2(-64)^k}=\frac{8(2n+1)}{(-64)^n}\binom{2n}{n}^3,$$

he deduced

$$\sum_{k=0}^{\infty}\frac{k(4k-1)\binom{2k}{k}^3}{(2k-1)^2(-64)^k}=-\frac{1}{\pi}. \tag{1}$$

We aim to give a systematic method to construct series like (1). This motivates us to consider the following problem: Given a hypergeometric term t_k, for which rational functions $r(k)$ is the product $r(k)t_k$ Gosper summable?

By aid of Gosper's algorithm, we give candidates for the denominator of $r(k)$. Then by polynomial reduction [2,4], we derive an upper bound and a lower bound on the degree of the numerator of $r(k)$. Based on these results, we are able to construct several new series involving π.

Wang and Zhong [6] further extended the method of polynomial reduction to P-recursive sequences. We also give a brief introduction on their results.

The second one focuses on the congruences of partial sums of P-recursive sequences [3]. For example, we have

$$\frac{2}{n}\sum_{k=1}^{n}(2k+1)M_k^2\in\mathbb{Z}.$$

where

$$M_k = \sum_{l=0}^{k} \binom{k}{2l} \frac{\binom{2l}{l}}{l+1}$$

is the k-th Motzkin number.

Let $\{a_k^{(i)}\}_{k\geq 0}, (1 \leq i \leq m)$ be P-recursive sequences of order d_i, respectively. We aim to find non-trivial polynomials $X(k)$ and $A_{i_1,\ldots,i_m}(k)$ such that

$$X(k)a_k^{(1)} \cdots a_k^{(m)} = \Delta \left(\sum_{(i_1,\ldots,i_m)\in S} A_{i_1,\ldots,i_m}(k) a_{k-i_1}^{(1)} \cdots a_{k-i_m}^{(m)} \right).$$

Summing over k from 0 to $n-1$ and considering the congruences of boundary values, we will derive the congruence of

$$\sum_{k=0}^{n-1} X(k) a_k^{(1)} \cdots a_k^{(m)}.$$

Keywords
telescoping, Gosper's algorithm, congruence

References

[1] G. BAUER, Von den Coefficienten der Reihen von Kugelfunctionen einer Variablen. *J. Reine Angew. Math.* **56**, 101–121 (1859).
[2] S. CHEN; H. HUANG; M. KAUERS; Z. LI, A modified Abramov-Petkovšek reduction and creative telescoping for hypergeometric terms. In *Proceedings of the 2015 ACM on International Symposium on Symbolic and Algebraic Computation*, 117–124. ACM, Bath, 2015.
[3] Q.-H. HOU; K. LIU, Congruences and telescopings of P-recursive sequences, *J. Difference Equ. Appl.* **27**(5), 686–697 (2021).
[4] Q.-H. HOU; Y.-P. MU; D. ZEILBERGER, Polynomial reduction and supercongruences. *J. Symbolic Comput.* **103**, 127–140 (2021).
[5] Z.-W. SUN, New series for powers of π and related congruences, *Electron. Res. Arch.* **28**(3), 1273–1342 (2020).
[6] R.-H. WANG; M.X.X. ZHONG, Polynomial reduction for holonomic sequences and applications in π-series and congruences, arXiv: 2205.11129.

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session *"D-Finite Functions and Beyond: Algorithms, Combinatorics, and Arithmetic"*

A symbolic-numeric validation algorithm for linear ODEs with Newton-Picard method

Florent Bréhard[1]***, Nicolas Brisebarre***[2]***, Mioara Joldes***[3] [florent.brehard@univ-lille.fr]

[1] Université de Lille, CNRS, Centrale Lille, UMR 9189 CRIStAL, France
[2] CNRS, LIP, Inria AriC, Université de Lyon, France
[3] LAAS-CNRS, Université de Toulouse, CNRS, France

Computing uniform approximations with validated error bounds for solutions of various kinds of differential equations is a very common task in the community of computer-assisted proofs in mathematics [1, 2, 3, 4].

Spectral-Galerkin methods are a tool of choice for computing uniform approximations of the solution of a linear ordinary differential equation [5, 6, 7]. The variable coefficients as well as the solution are approximated by truncated series in a well-chosen chosen basis of orthogonal functions, like the Chebyshev polynomials. The idea is to rephrase the differential equation as an infinite linear system and solve a finite-dimensional truncation of it, thanks to some compactness property. It is therefore natural to consider the same truncation scheme to design a Newton-like a posteriori validation operator [8, 9, 10]. Using the Banach fixed-point theorem, one obtains a rigorous error bound associated to the approximation obtained by the numerical spectral method.

In the first part of this talk, we will show that although spectral methods are known to produce exponentially fast convergent approximations, the corresponding validation procedure may converge much slower [10]. Indeed, the truncation index for the validation operator may be much larger than the one actually used for numerical approximation in the spectral method, rapidly leading to very large matrices.

In the second part of this talk, we present an alternative validation algorithm [11] with the desired "exponential convergence" property. Inspired by the famous Picard iterations [12], the idea consists in approximating the so-called "resolvent kernel" of the inverse integral operator rather than truncating the corresponding infinite matrix. It is similar in essence to the symbolic Newton iterations on differential equations [13, 14, 15], but in a numerical setting in a well-chosen Banach space of coefficients of orthogonal functions rather than exact Taylor expansions. This complexity gap is illustrated in practice by examples involving "large" parameters.

Keywords
Linear Differential Equations, Validated Numerics, Spectral Methods

References

[1] W. TUCKER, A rigorous ODE solver and Smale's 14th problem. *Foundations of Computational Mathematics* **2**, 53–117 (2002).
[2] M. T. NAKAO; M. PLUM; Y. WATANABE, *Numerical Verification Methods and Computer-Assisted Proofs for Partial Differential Equations*. Springer, 2019.
[3] D. WILCZAK; P. ZGLICZYŃSKI, C^r-Lohner algorithm. *Schedae Informaticae* **20**, 9–42 (2011).
[4] J. B. VAN DEN BERG; J.-P. LESSARD, Rigorous numerics in dynamics. *Notices of the AMS* **62**(9) (2015).
[5] D. GOTTLIEB; S. A. ORSZAG, *Numerical Analysis of Spectral Methods: Theory and Applications*. SIAM, 1977.
[6] J. P. BOYD, *Chebyshev and Fourier spectral methods*. Dover Publications, 2001.
[7] S. OLVER; A. TOWNSEND, A fast and well-conditioned spectral method. *SIAM Review* **55**(3), 462–489 (2013).
[8] N. YAMAMOTO, A numerical verification method for solutions of boundary value problems with local uniqueness by Banach's fixed-point theorem. *SIAM Journal of Numerical Analysis* **35**(5), 2004–2013 (1998).
[9] J.-P. LESSARD; C. REINHARDT, Rigorous numerics for nonlinear differential equations using Chebyshev series. *SIAM Journal of Numerical Analysis* **52**(1), 1–22 (2014).
[10] F. BRÉHARD; N. BRISEBARRE; M. JOLDES, Validated and numerically efficient Chebyshev spectral methods for linear ordinary differential equations. *ACM Transactions on Mathematical Software* **44**(4), 44:1–44:42 (2018).
[11] F. BRÉHARD, A Symbolic-Numeric Validation Algorithm for Linear ODEs with Newton-Picard Method. *Mathematics in Computer Science* **15**(3), 373–405.
[12] T. LALESCU, *Introduction à la Théorie des Équations Intégrales (Introduction to the Theory of Integral Equations)*. Librairie Scientifique A. Hermann, 1911.
[13] R. P. BRENT; H. T. KUNG, Fast algorithms for manipulating formal power series. *Journal of the ACM* **25**(4), 581–595 (1978).
[14] A. BOSTAN; F. CHYZAK; F. OLLIVIER; B. SALVY; É. SCHOST; A. SEDOGLAVIC, Fast computation of power series solutions of systems of differential equations. In *ACM-SIAM Symposium on Discrete Algorithms*, 2006.
[15] J. VAN DER HOEVEN, Newton's method and FFT trading. *Journal of Symbolic Computation* **45**(8), 857–878 (2010).

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session *"D-Finite Functions and Beyond: Algorithms, Combinatorics, and Arithmetic"*

Algebraic consequences of the fundamental theorem of calculus in differential rings

Clemens G. Raab[1]**, *Georg Regensburger***[2] `[regensburger@mathematik.uni-kassel.de]`

[1] Institute for Algebra, Johannes Kepler University Linz, Austria
[2] Institute of Mathematics, University of Kassel, Germany

In this talk, we discuss the fundamental theorem of calculus and its consequences from an algebraic point of view [1]. In particular, for functions with singularities, this leads to a generalized notion of evaluation. We present properties of such integro-differential rings and discuss several examples. We outline the construction of the corresponding integro-differential operators and provide normal forms using rewrite rules. These rewrite rules are then used to derive several identities and properties in a purely algebraic manner, generalizing well-known results from analysis. In identities such as shuffle relations for nested integrals and the Taylor formula, additional terms are obtained to account for singularities. Another focus lies on treating the basics of linear ordinary differential equations (ODEs) within the framework of integro-differential operators. These operators can have matrix coefficients, enabling the treatment of systems of arbitrary size in a unified manner.

Keywords
Integro-differential rings, integro-differential operators, normal forms, generalized shuffle relations, generalized Taylor formula

References

[1] CLEMENS G. RAAB; GEORG REGENSBURGER, The fundamental theorem of calculus in differential rings. *arXiv:2301.13134 [math.RA]* (2023).

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session *"D-Finite Functions and Beyond: Algorithms, Combinatorics, and Arithmetic"*

Separating variables in bivariate polynomial ideals: the local case

Manfred Buchacher[1] [manfredi.buchacher@gmail.com]

[1] RICAM, Austrian Academy of Sciences, Linz, Austria

We report on work in progress on the problem of finding all elements of $\mathbb{K}(x) + \mathbb{K}(y)$ that are of the form qp for a given irreducible polynomial $p \in \mathbb{K}[x, y]$ and some non-zero rational function $q \in \mathbb{K}(x, y)$ whose denominator is not divisible by p.

Let p be an irreducible polynomial of $\mathbb{K}[x, y]$ that is not an element of $\mathbb{K}[x] \cup \mathbb{K}[y]$. We define the *local ring* of $\mathbb{K}[x, y]$ at p by

$$\mathbb{K}[x, y]_p := \{r \in \mathbb{K}(x, y) : p \nmid \operatorname{denom}(r)\}.$$

and denote by $\langle p \rangle$ the set of multiples of p in $\mathbb{K}[x, y]_p$. The set of *separated multiples* of p is

$$\langle p \rangle \cap (\mathbb{K}(x) + \mathbb{K}(y))$$

and can be described by

$$\mathrm{F}(p) := \{(f, g) \in \mathbb{K}(x) \times \mathbb{K}(y) : f - g \in \langle p \rangle\}.$$

The latter is a field with respect to component-wise addition and multiplication and referred to as the *field of separated multiples* of p. By Lüroth's theorem there is a pair $(f, g) \in \mathbb{K}(x) \times \mathbb{K}(y)$ of rational functions such that

$$\mathrm{F}(p) = \mathbb{K}((f, g)).$$

If there are $f \in \mathbb{K}(x)$ and $g \in \mathbb{K}(y)$ such that $qp = f - g$ for some $q \in \mathbb{K}(x, y) \setminus \{0\}$, then it is enough to know the singularities of f and g and their multiplicities to find them. The latter essentially means to know the denominators of f, g and q and the degrees of their numerators. The unknown f, g and q can then be determined by making an ansatz for their numerators, clearing denominators in $qp = f - g$, comparing coefficients and solving a system of linear equations for them. We present a heuristic to determine the singularities of f and g and their multiplicities by inspecting the leading parts of p with respect to different gradings. Based on previous work [1] we also explain why we belief that our reasoning gives rise to an algorithm that solves the problem of determining a $(f, g) \in \mathbb{K}(x) \times \mathbb{K}(y)$ that generates $\mathrm{F}(p)$.

Keywords
Commutative algebra, elimination theory, separation of variables

References

[1] MANFRED BUCHACHER, MANUEL KAUERS, GLEB POGUDIN, *Separating variables in bivariate polynomial ideals.* Proceedings of the 45th International Symposium on Symbolic and Algebraic Computation, 54–61, 2020.

[2] OLIVIER BERNARDI, MIREILLE BOUSQUET-MÉLOU, KILIAN RASCHEL, *Counting quadrant walks via Tutte's invariant method.* Discrete Mathematics & Theoretical Computer Science, 2020.

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17 – 21, 2023
Session on *"Computer Algebra Systems and Interval Methods"*

On an application of an interval finite difference method for solving the heat conduction problem

Malgorzata A. Jankowska[1]***, Bartłomiej Jacek Kubica***[2]***,***
Andrzej Marciniak[3,4]***, Tomasz Hoffmann***[5]
[malgorzata.jankowska@put.poznan.pl]

[1] Institute of Applied Mechanics, Poznan University of Technology, Poznan, Poland
[2] Institute of Information Technology, Warsaw University of Life Sciences – SGGW, Warsaw, Poland
[3] Institute of Computing Science, Poznan University of Technology, Poznan, Poland
[4] Department of Computer Science, Higher Vocational State School in Kalisz, Kalisz, Poland
[5] Poznan Supercomputing and Networking Center, Poznan, Poland

Obtaining interval enclosures for the solutions of partial differential equations (PDE) is not a simple task. Several researchers have proposed various methods of bounding the solution functions (see, e.g. [4]). The authors of this study propose the interval method for solving a parabolic partial differential equation known as the heat equation of the form:

$$\frac{\partial u}{\partial t}(x,t) - \alpha^2 \frac{\partial^2 u}{\partial x^2}(x,t) = 0, \quad 0 < x < L,\ t > 0, \tag{1}$$

with the following initial and boundary conditions:

$$u(x,0) = f(x), \quad 0 \le x \le L,$$
$$u(0,t) = \varphi_1(t), \quad u(L,t) = \varphi_2(t), \quad t > 0.$$

The finite difference schemes are used to obtain the required interval formulas and then the interval realization of very effective variety of direct Cholesky method is applied for solving the system of linear equations of the special positive definite, tridiagonal and symmetric matrices. The interval method shown in the paper includes the error term of the corresponding conventional method. In the theoretical approach presented this error is bounded by some interval values. Together with interval floating-point arithmetic it allows the user to obtain a guaranteed result. The theoretical considerations are supported by results of some numerical experiments. Note that the authors are going to investigate the use of symbolic methods for the purpose of improving the accuracy and efficiency of the interval methods [1-4].

Keywords
interval computations, partial differential equations, heat equation, finite differences, symbolic transformation

References

[1] Jankowska, M.A., Marciniak, A., Hoffmann, T. On an Application of an Interval Backward Finite Difference Method for Solving the One-Dimensional Heat Conduction Problem. *Control and Cybernetics* **44(4)**, 463-480 (2015).

[2] B. J. Kubica, Algorithmic differentiation and hull-consistency enforcing using C++ template meta-programming. *Numerical Algorithms Journal*, accepted, DOI: 10.1007/s11075-023-01551-8.

[3] B. J. Kubica, *Interval methods for solving nonlinear constraint satisfaction, optimization and similar problems: From inequalities systems to game solutions*. Springer, Cham, Switzerland, 2019, DOI: 10.1007/978-3-030-13795-3.

[4] Nakao, M. T., Plum, M., and Watanabe, Y., Numerical Verification Methods and Computer-Assisted Proofs for Partial Differential Equations.*Springer Singapore* (2019).

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session *"Computer Algebra Systems and Interval Methods"*

On the application of directed interval arithmetic for solving elliptic BVP

Tomasz Hoffmann[1]***, Andrzej Marciniak***[2,3]***, Malgorzata A. Jankowska***[4]
[tomhof@man.poznan.pl]

[1] Poznan Supercomputing and Networking Center, Poznan, Poland
[2] Institute of Computing Science, Poznan University of Technology, Poznan, Poland,
[3] Department of Computer Science, Higher Vocational State School in Kalisz, Kalisz, Poland
[4] Institute of Applied Mechanics, Poznan University of Technology, Poznan, Poland

The properties of directed interval arithmetic are interesting, as due to the existence of the opposite and inverse element, it allows us to perform computations in a way that enables a certain reduction in the width of the end-intervals – the solution. We performed experiments to solve some elliptic boundary value problems, which confirmed that the intervals obtained after applying this arithmetic are narrower than in the case of proper interval arithmetic. An attempt is also made to refer to a method that allows a rigorous verification of the existence of PDE solutions and finding their estimate supported by mathematical proof. Such a method for elliptic equations is the Nakao method using the FEM model. The results obtained with both types of methods, i.e. the proposed interval methods and the interval-based (but not fully interval) Nakao method, were compared.

Keywords
Directed Interval Arithmetic, Boundary Value Problem, Finite Difference Methods, Verified Computing

References
[1] MARKOV, S., On Directed Interval Arithmetic and Its Applications. *he Journal of Universal Computer Science* pp. 515–526, Springer (1996).
[2] NAKAO, M. T., A Numerical Approach to the Proof of Existence of Solutions for Elliptic Problems. *Japan Journal of Applied Mathematics* **5**(2), p.313 (1988).
[3] NAKAO, M. T., PLUM, M., AND WATANABE, Y., Numerical Verification Meth- ods and Computer-Assisted Proofs for Partial Differential Equations.*Springer Singapore* (2019).
[4] POPOVA, E. D., Extended Interval Arithmetic in IEEE Floating-Point Environmen. *Interval Computations* **4**, pp. 100–129 (1994).

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session *"Computer Algebra Systems and Interval Methods"*

Symbolic and algorithmic differentiation for the interval algorithm of training contracting autoencoders

Bartłomiej Jacek Kubica[1] [bartlomiej_kubica@sggw.edu.pl]

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

Autoencoders (AE) are a specific kind of unsupervised (or semi-supervised) feed-forward neural networks.

The AE consists of at least three layers: the input layer (x), the hidden layer (h), and the output layer (y). Its essence is to reproduce the input on the output, but not in a trivial manner: $y = x$, but approximately. Depending on the structure and dimensionality of the hidden layer, the input can be reconstructed more or less precisely, and – as we shall see – the reconstruction process will capture various features of the data.

An AE can be logically decomposed into two parts:

- the *encoder*, transforming the input x to the representation of data, in the hidden layer: $h = f(x)$,
- the *decoder*, transforming the representation to the data from the original space: $y = f^*(h)$.

The f^* function in the above description is some sort of an 'approximate inverse' of f.

A specific kind of AEs are contractive autoencoders (CAE). Their essence is to train the AE so that we had $h = f(x)$, and the derivative of f was close to zero at the training points. Usually, it is obtained by adding the the loss function a regularization term, penalizing a norm of the Jacobi matrix of f.

Why would an AE satisfy such a condition? What do derivatives close to zero imply?

The idea is pretty similar (but not mathematically equivalent!) to a denoising AEs: when the derivative of f is close to zero, adding a noise to x does not change its representation significantly.

In the paper, an interval approach [1] to training such AEs is going to be presented. The method is similar to the one from [2], and it is directly based on the one described in [3], but now it is necessary to seek points for whichthe gradient of a given function is close to zero.

For this purpose, hull-consistency (HC) enforcing procedures from ADHC 2.2 [4] are not sufficient. These procedures allow to enforce HC for a function, but not for its derivative(s).

A novel procedure is presented, performing symbolic transformations of the expression tree generated by ADHC. Hence, we obtain the new expression tree(s), representing the derivative(s) of the function under consideration; now, HC can be enforced on the gradient-related constraints.

Keywords
interval computations, constraint satisfaction, algorithmic differentiation, symbolic differentiation, contractive auto-encoders

References

[1] B. J. KUBICA, *Interval methods for solving nonlinear constraint satisfaction, optimization and similar problems: From inequalities systems to game solutions*. Springer, Cham, Switzerland, 2019, DOI: 10.1007/978-3-030-13795-3.
[2] B. J. KUBICA; P. HOSER; A. WILIŃSKI, Interval methods for seeking fixed points of recurrent neural networks. In *International Conference on Computational Science*, 414–423, Springer, 2020.
[3] B. J. KUBICA, Developing an interval method for training denoising autoencoders by bounding the noise. Submitted.
[4] B. J. KUBICA, Algorithmic differentiation and hull-consistency enforcing using C++ template meta-programming. *Numerical Algorithms Journal*, accepted, DOI: 10.1007/s11075-023-01551-8.

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17 – 21, 2023
Session on *"Computer Algebra Systems and Interval Methods"*

Symbolic recipes for solving nonlinear systems of equations with interval methods

Laurent Granvilliers[1] [laurent.granvilliers@univ-nantes.fr]

[1] LS2N, Nantes Université, France

Interval branch-and-prune algorithms are able to find all the solutions of a nonlinear system of equations and to certify the results [1]. To this end, they combine branching steps and reduction techniques like local consistency techniques, constraint propagation, the interval Newton operator, and linear relaxation based methods. At different levels, all these techniques strongly depend on the symbolic expressions of nonlinear systems that may lead to pessimistic interval computations. In this talk, we will review some of these methods along with expression sharing in directed acyclic graphs [2] and symbolic rewriting of expressions and systems [3]. We will study the specifc problem of finding all the roots of a complex polynomial using trigonometric forms.

Keywords
Branch-and-prune algorithm, nonlinear equations, symbolic rewriting

References

[1] P. Van Hentenryck, D. McAllester, D. Kapur, Solving polynomial systems using a branch and prune approach. *SIAM Journal on Numerical Analysis* **34**(2), 797–827 (1997).
[2] H. Schichl, A. Neumaier , Interval Analysis on Directed Acyclic Graphs for Global Optimization. *Journal of Global Optimization* **33**(1), 541–562 (2005).
[3] F. Benhamou, L. Granvilliers, Combining Local Consistency, Symbolic Rewriting and Interval Methods. In *Proceedings of the International Conference on Artificial Intelligence and Symbolic Mathematical Computation (AISMC-3), Lecture Notes in Computer Science 1138*, J. Calmet, J. A. Campbell, J. Pfalzgraf (eds.), 144–159. Springer-Verlag, Steyr, Austria, 1996.

Applications of Computer Algebra – ACA 2023
Warsaw. Poland | July 17-21, 2023
Session on *"Computer Algebra Applications in the Life Sciences"*

Inferring stochastic models of gene transcription from initiation events by computer algebra

Ovidiu Radulescu[1] [ovidiu.radulescu@umontpellier.fr]

[1] University of Montpellier 2, Montpellier, France

Gene transcription regulation can be modelled using finite state Markov chains. Through live imaging experiments, we obtain the sequence of transcription initiation events and find the distribution of the time between events, the so-called phase-type distribution. We discuss the following inverse problem: knowing the phase-type distribution, can we determine the transition rate parameters of the Markov chain? In the non-degenerate case when the characteristic equation of the transition matrix has distinct eigenvalues, the phase-type distribution is multi-exponential. We reduce inverse problem to a system of polynomial equations whose coefficients are symmetric polynomials in the parameters of the multiexponential distribution. For special Markov chains this system has unique solutions expressed as rational symmetric functions of the distribution parameters. We use the algebraic Thomas decomposition to find solutions for all the three and four states Markov chain models. Analysis of the inverse problem shows that multiple interpretations of the data are possible, a phenomenon known as the "Rashomon effect": different Markov chain models predict exactly the same phase-type distribution.

Keywords
Gene transcription

Applications of Computer Algebra – ACA 2023
Warsaw. Poland | July 17-21, 2023
Session on *"Computer Algebra Applications in the Life Sciences"*

Duality in mass-action networks

Alexandru Iosif[1] [alexandru.iosif@urjc.es]

[1] Applied Mathematics Area, Rey Juan Carlos University, Madrid, Spain

We introduce maximal invariant polyhedral supports and, for conservative mass-action networks that do not have two species with exactly the same rates, we prove that the set of preclusters is dual to the set of maximal invariant polyhedral supports. Precusters are special cases of the clusters introduced in 2012 by Conradi and Flockerzi [1]. In author's thesis [2] it is given, in terms of precusters, a sufficient condition for the existence of positive steady states. Given the close relation between maximal invariant polyhedral supports and siphons, we conjecture that there is a duality relation between siphons and clusters, which, we belive, based on [3], might lead to uniqueness of Birch points in systems with small codimensional invariant polyhedra.

Keywords
Mass-action networks, Birch points, Siphons

References

[1] C. Conradi and D. Flockerzi, Multistationarity in mass action networks with applications to ERK activation. *Journal of mathematical biology* **volume**(65), no. 1, 107–156 (2012).
[2] A. Iosif, *Algebraic methods for the study of multistationarity in mass- action networks*. Ph.D. thesis, Otto-von-Guericke-Universität Magdeburg, 2019.
[3] A. Shiu, *Algebraic methods for biochemical reaction network theory*. Ph.D. thesis, University of California, Berkeley, 2010.

Applications of Computer Algebra – ACA 2023
Warsaw. Poland | July 17-21, 2023
Session on *"Computer Algebra Applications in the Life Sciences"*

Phylogenetic invariants for time-reversible models

***Marta Casanellas*[1,2]*, Roser Homs Pons*[1]*, Angélica Torres*[1]** [atorres@crm.cat]

[1] Centre de Recerca Matemàtica, Bellaterra, Barcelona, Spain
[2] Universitat Politècnica de Catalunya, Barcelina, Spain

The main goal of Phylogenetics is to find evolutionary relations between biological entities. These relations are inferred from data and are encoded in a graph called a *phylogenetic tree*. The leaves of a phylogenetic tree represent the observed species, and each interior node corresponds to a common ancestor of the species descending from it.

Available data can come from DNA sequences or aminoacid sequences of different species, but once we have the data ¿How to determine which phylogenetic tree accurately represents the evolutionary relations hidden in the data? Generally there are two steps to solve this question: Model selection and phylogenetic reconstruction. On the first step the main goal is to decide how the transition of species occurs, and on the second step the goal is to build the phylogenetic tree.

In this talk we explore how understanding the phylogenetic variety helps us both with model selection and phylogenetic reconstruction. We will start by introducing phylogenetic varieties and time-reversible models, then we present a general framework to study the phylogenetic reconstruction process for time-reversible models. Our main example will be the Tamura Nei model for DNA, for which we give phylogenetic invariants that allow us to distinguish whether a tree fits the data when the evolution occurs under a time-reversible model.

This is joint work with Marta Casanellas and Roser Homs Pons.

Keywords
phylogenetic invariants, time-reversible models, phylogenetic variety

Applications of Computer Algebra – ACA 2023
Warsaw. Poland | July 17-21, 2023
Session on *"Computer Algebra Applications in the Life Sciences"*

Divide & Control: an efficient decomposition-based approach towards the control of asynchronous boolean networks

Andrzej Mizera[1,2] [andrzej.mizera@ideas-ncbr.pl]

[1] IDEAS-NCBR, Warsaw, Poland
[2] Institute of Informatics, University of Warsaw

We consider the problem of computing a minimal subset of nodes of a given asynchronous Boolean network that perturbed in a single-step drive its dynamics from an initial state to a target attractor. We refer to this problem as the source-target control of Boolean networks. Due to the infamous phenomenon of state-space explosion, a global approach that performs computations on the entire network may not scale well for large networks. We take the view that efficient control algorithms for such networks must exploit both the structure and dynamics of the networks. With this, we derive a decomposition-based solution to the minimal source-target control problem and we show that it can be significantly faster than the existing approaches on large networks. We apply our solutions to both real-life biological networks and randomly generated networks, demonstrating the efficiency and efficacy of our approach.

Keywords
Gene regulatory networks, Boolean networks, Attractors, Network control

Applications of Computer Algebra – ACA 2023
Warsaw. Poland | July 17-21, 2023
Session on *"Computer Algebra Applications in the Life Sciences"*

Gene regulatory network inference with joint multi-omic single-cell data to learn dynamic cell state transitions

Adam L. MacLean[1] [macleana@usc.edu]

[1]Department of Quantitative and Computational Biology, USC Dornsife College of Letters, Arts and Sciences, University of Southern California, Los Angeles, California, US

Single-cell genomics offer unprecedented resolution with which to study cell fate decision-making. We present new tools to infer gene regulatory networks (GRNs) controling cell fate decisions and model their multiscale dynamics. We introduce popInfer, single-cell multi-modal GRN inference via regularized regression, and demonstrate its potential for network discovery. Through application to hematopoiesis, we discover new gene interactions regulating early fate decisions during stem cell differentiation that are profoundly affected by diet and age.

Keywords
gene regulatory networks, multiscale dynamics, hematopoiesis, statistical inference

Applications of Computer Algebra – ACA 2023
Warsaw. Poland | July 17-21, 2023
Session on *“Computer Algebra Applications in the Life Sciences”*

Five equivalent representations of a phylogenetic tree

Jiayue Qi[1], ***Josef Schicho***[1] [jiayue.qi@dk-compmath.jku.at]

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

A phylogenetic tree is a tree with a fixed set of leaves that has no vertices of degree two. To our knowledge, there are four other representations of such a tree: sets of partitions, sets of cuts, crossing relations, and equivalences of triples. In this paper, we focus on these four representations, and show that they are all equivalent. In particular, we give the conversions in between them, which builds the bridges that eventually connect the five representations.

Keywords
phylogenetic tree, equivalent representations, conversions between different representations

Applications of Computer Algebra – ACA 2023
Warsaw. Poland | July 17-21, 2023
Session on *"Computer Algebra Applications in the Life Sciences"*

Computing sign vector conditions for existence and uniqueness of equilibria of chemical reaction networks

Marcus Aichmayr[1]***, Georg Regensburger***[1] [aichmayr@mathematik.uni-kassel.de]

[1] Institute of Mathematics, University of Kassel, Germany

In [1], conditions for existence and uniqueness of equilibria of chemical reaction networks with generalized mass-action kinetics for all parameters are introduced. The conditions for uniqueness and (robust) existence are formulated in terms of sign vectors of subspaces corresponding to the stoichiometric coefficients and the kinetic orders of the reactions. In this talk, we will discuss how these sign vector conditions can be checked algorithmically, utilizing techniques based on oriented matroids. We illustrate our methods by examples of chemical reaction networks with generalized mass-action kinetics using our implementation in SageMath [2].

Keywords
sign vectors, oriented matroids, robustness, generalized mass-action kinetics, deficiency zero theorem

References
[1] S. MÜLLER, J. HOFBAUER, G. REGENSBURGER, On the bijectivity of families of exponential/generalized polynomial maps. *SIAM Journal on Applied Algebra and Geometry* **3**(3), 412–438 (2019).
[2] M. AICHMAYR, Computing with sign vectors in SageMath and applications to exponential maps. *Master's thesis, Johannes Kepler University Linz.* 2021.

Applications of Computer Algebra – ACA 2023
Warsaw. Poland | July 17-21, 2023
Session on *“Computer Algebra Applications in the Life Sciences”*

How to find or exclude bifurcations in biochemical systems?

Nicola Vassena [nicola.vassena@uni-leipzig.de]

Leipzig University

Bifurcation theory is a standard method to detect dynamical behaviors of interest, such as multistationarity and oscillations. The localization of bifurcations in large parametric systems still requires both rigorous criteria and some informal intuition. In this talk we present a symbolic approach based only on an algebraic analysis of the Jacobian matrix. The spectral configuration of the Jacobian matrix at an equilibrium is a necessary condition for a certain bifurcation to happen. For example, a simple eigenvalue zero points at saddle-node bifurcations and consequent multistationarity, while purely imaginary eigenvalues hint at Hopf bifurcations and oscillatory behavior.

We investigate how the network structure infers the spectrum of the Jacobian. We show that such an approach is effective to *detect* zero or purely-imaginary eigenvalues for systems endowed with Michaelis-Menten kinetics and Hill kinetics. Moreover, the same approach can be also used to *exclude* bifurcations for systems endowed with mass action, Michaelis-Menten, and Hill kinetics. The talk is based on results from [1] and [2].

Keywords
Chemical reaction networks, Bifurcation analysis, Symbolic approach, Michaelis-Menten kinetics, Function-free

References
[1] N. VASSENA, Symbolic hunt of instabilities and bifurcations in reaction networks. arXiv: 2303.03089, Submitted (2023).
[2] N. VASSENA, Structural conditions for saddle-node bifurcations in chemical reaction networks. *To appear in SIAM J. Appl. Dyn. Syst.* .

Applications of Computer Algebra – ACA 2023
Warsaw. Poland | July 17-21, 2023
Session on *"Computer Algebra Applications in the Life Sciences"*

Generic dimension of varieties arising in reaction network theory and 3D genome reconstruction

Oskar Henriksson[1] [oskar.henriksson@math.ku.dk]

[1] Department of Mathematical Sciences, University of Copenhagen, Denmark

Systems of polynomial equations with unknown parameters appear in many biological contexts, and a common theme in applied algebraic geometry is to investigate how various geometrical properties of the solution set vary with the parameters. One of the most fundamental such properties is the dimension, and in this talk, I will discuss various algebraic methods for determining the *generic dimension*, based on the concept of nondegenerate solutions – also for systems that are too large for standard Gröbner basis techniques to be feasible.

Two biological applications will be highlighted. First, we will focus on steady state varieties in reaction network theory, for which we in [3] find computational criteria for when the generic codimension coincides with the rank of the network. As a corollary, we prove that under the assumption of mass action kinetics, all weakly reversible networks have finitely many steady states for generic rate constants and any total concentrations, which settles a question posed by Boros, Craciun and Yu in [1]. Finally, we turn to the problem of 3D genome reconstruction, where we in [2] employ similar techniques to computationally prove finite identifiability from Hi-C data for diploid organisms, provided that maternal and paternal DNA sequences can be distinguished for a small number of genomic loci [2].

This is a combination of joint works with Diego Cifuentes, Jan Draisma, Elisenda Felu, Annachiara Korchmaros, Kaie Kubjas and Beatriz Pascual-Escudero.

Keywords
parametric polynomial systems, generic dimension, reaction networks, 3D genome reconstruction, identifiability

References

[1] B. Boros, G. Craciun, and P. Y. Yu, Weakly reversible mass-action systems with infinitely many positive steady states. *SIAM J. Appl. Math*, **80**(4), 1936–1946 (2020).
[2] D. Cifuentes, J. Draisma, O. Henriksson, A. Korchmaros and K. Kubjas, 3D genome reconstruction from partially phased Hi-C data. ArXiv preprint: 2301.11764 [q-bio.GN] (2023).
[3] E. Feliu, O. Henriksson and B. Pascual-Escudero, Dimension and degeneracy of solutions of parametric polynomial systems arising from reaction networks. ArXiv preprint: 2304.02302 [math.AG] (2023).

Applications of Computer Algebra – ACA 2023
Warsaw. Poland | July 17-21, 2023
Session on *"Computer Algebra Applications in the Life Sciences"*

Hopf bifurcations in some biochemical models

Valery G. Romanovski[1,2] [valerij.romanovskij@um.si]

[1] Faculty of Electrical Engineering and Computer Science and Faculty of Natural Science and Mathematics, University of Maribor, Maribor, Slovenia
[2] Center for Applied Mathematics and Theoretical Physics, University of Maribor, Maribor, Slovenia

Existence of periodic oscillations is an important feature of various chemical reaction models. The most common method to find such bifurcations is the investigation of Hopf bifurcations. We discuss an approach based on the elimination theory of computational algebra to find conditions for the existence of Hopf bifurcations in polynomial systems of ordinary differential equations.

We apply the approach to study limit cycle bifurcations in a three-dimensional Lotka-Volterra system which models a food web of three species, one of which is an omnivore. For the model we first find necessary and sufficient conditions for existence of a pair of pure imaginary eigenvalues for the Jacobian of the system at the stationary point with positive coordinates. Then it is shown that the system can have two small limit cycles bifurcating from the singular point.

Models related to the double phosphorylation of mitogen-activated protein kinases are discussed as well.

Keywords
Biochemical reactions, Hopf bifurcation, Center manifold, Limit cycle, Elimination ideal

References

[1] Y. LI AND V. G. ROMANOVSKI, Hopf bifurcations in a Predator-Prey Model with an Omnivore. *Qual. Theory Dyn. Syst.* **18**, 1201–1224 (2019).
[2] C. PANTEA AND V. G. ROMANOVSKI, Qualitative study of some biochemical models,Bifurcations in a closed-loop. *Vestn. St. Petersb. Univ. Math.* **53**, 214–222 (2020).

Applications of Computer Algebra – ACA 2023
Warsaw. Poland | July 17-21, 2023
Session on *"Computer Algebra Applications in the Life Sciences"*

CAD adjacency computation using validated numerics

Adam Strzebonski[1] [adams@wolfram.com]

[1] Wolfram Research, Champaign, Illinois, United States

We will present an algorithm for computation of cell adjacencies for well-based cylindrical algebraic decomposition. The algorithm determines cell adjacency information using validated numerical methods similar to those used in CAD construction, thus computing CAD with adjacency information in time comparable to that of computing CAD without adjacency information. Our implementation in Mathematica uses cell adjacency information to compute topological operations e.g. closure, boundary, and connected components. Other applications include computing topological properties e.g. homology groups, visualization and path planning.

Keywords
Cylindrical Algebraic Decomposition, cell adjacency, topology of semialgebraic sets, connected components

References

[1] A. STRZEBOŃSKI, CAD Adjacency Computation Using Validated Numerics. *ISSAC '17: Proceedings of the 2017 ACM on International Symposium on Symbolic and Algebraic Computation* , 413-420 (2017).

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session on *“Computational Difference and Differential Algebra and its Applications”*

Classifications of prime ideals and simple modules of the Weyl algebra A_1 in prime characteristic

V. V. Bavula[1] [v.bavula@sheffield.ac.uk]

[1] School of Mathematics and Statistics, University of Sheffield, Sheffield, UK

Let K is an arbitrary field of characteristic $p > 0$. Classifications of prime, completely prime, maximal and primitive ideals and simple modules are obtained for the Weyl algebra $A_1 = K\langle x, \partial : \partial x - x\partial = 1\rangle$, the skew polynomial algebra $\mathbb{A} = K[h][x; \sigma]$ and the skew Laurent polynomial algebra $\mathcal{A} := K[h][x^{\pm 1}; \sigma]$ where $\sigma(h) = h - 1$. The quotient rings (of fractions) of prime factor algebras of the algebras A_1, $\mathbb{A}$ and $\mathcal{A}$ are described. They are either fields or matrix algebras over *fields* or *cyclic* algebras.

Keywords
Weyl algebra, prime ideal, central simple algebra

References

[1] V. V. BAVULA, Classifications of prime ideals and simple modules of the Weyl algebra A_1 in prime characteristic. *Tokyo J. Math.l* **44**(1), 1–31 (2023).

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session on *"Computational Difference and Differential Algebra and its Applications"*

Multiplicity of arc spaces of fat points

***<u>Rida Ait El Manssour</u>*[1], *Gleb Pogudin*[2],** [rida.manssour@mis.mpg.de]

[1] Max Planck Institute for Mathematics in the Sciences, Inselstraße 22, 04103 Leipzig, Germany
[2] LIX, CNRS, École Polytechnique, Institute Polytechnique de Paris, 1 rue Honoré d'Estienne d'Orves, 91120, Palaiseau, France

Consider the algebraic equation $x^m = 0$, it defines a point on the affine line with multiplicity m. This corresponds to the dimension of the k-vector space $k[x]/\langle x^m\rangle$. If we consider the differential ideal of generated by x^m denoted by $\langle x^m\rangle^{(\infty)} \subseteq k[x^{(\infty)}]$, then this dimension is infinite (i.e. $\dim k[x^{(\infty)}]/\langle x^m\rangle^{(\infty)} = \infty$).

The infinite-dimensional algebra $k[x^{(\infty)}]/\langle x^m\rangle^{(\infty)}$ admits a natural filtration by finite dimensional algebras $k[\bar{x}, \bar{x'}, \ldots, \bar{x^{(h)}}]$. Therefore, we prove that $\dim k[\bar{x}, \bar{x'}, \ldots, \bar{x^{(h)}}] = m^{h+1}$ [1], which generalizes the concept of multiplicity to arc spaces. The proof of this result is based on determining the initial ideal of $\langle x^m\rangle^{(\infty)}$ with respect to lexicographical ordering. The description of the initial ideal was previously conjectured by Afsharijoo [2, Section 5], which serves in finding new partition identities generalizing Roger-Ramanujan identities.

At the end, we provide computational experiments for computing the growth multiplicities of the arc space of different zero-dimensional ideals.

Keywords
Arc space, Multiplicity, Gröbner basis

References
[1] R. AIT EL MANSSOUR, G. POGUDIN; Multiplicity structure of the arc space of a fat point. *ArXiv:* 2111.10446.
[2] P. AFSHARIJOO; Looking for a new Version of gordon's identities. *Annals of Combinatorics* 25, pages 543–571.

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session on *"Computational Difference and Differential Algebra and its Applications"*

A new type of difference Gröbner bases and their applications

Alexander Levin [levin@cua.edu]

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

Keywords
Difference module, effective order, Gröbner basis, dimension polynomial

We introduce a new type of Gröbner bases in free difference modules that are associated with a reduction respecting the effective order of module elements. (We generalize the notion of effective order of an ordinary difference polynomial (see [1, Chapter 2, Section 4]) to free difference modules with several translations.) Then we establish some properties of such Gröbner bases and present a Buchberger-type algorithm for their computation. Using the obtained results, we prove the existence and give a method of computation of a bivariate dimension polynomial of a finitely generated difference module that carries more module invariants than the univariate difference dimension polynomial introduced in [3] and studied in [2], [4] and in a number of papers. We also show how the new invariants can be applied to the isomorphism problem for difference modules and to the equivalence problem for systems of algebraic difference equations.

References

[1] R. M. COHN, *Difference Algebra*. Interscience, 1965.
[2] M. V. KONDRATEVA, A. B. LEVIN, A. V. MIKHALEV, AND E. V. PANKRATEV, *Differential and Difference Dimension Polynomials*. Kluwer Acad. Publ., 1999.
[3] A. B. LEVIN, Characteristic Polynomials of Filtered Difference Modules and of Difference Field Extensions. *Russian Math. Surveysl* **33**(1978), no. 3, 165–166.
[4] A. B. LEVIN, *Difference Algebra*. Springer, 2008.

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session on *"Computational Difference and Differential Algebra and its Applications"*

On the Schmidt–Kolchin conjecture

Antoine Etesse[1] [antoine.etesse@ens-lyon.fr]

[1] Institut de Mathématiques de Toulouse, Université Paul Sabatier, Toulouse, France

In this talk, we will discuss the Schmidt–Kolchin conjecture on differentially homogeneous polynomials, that we recently proved in [1]. This conjecture predicts that the vector space of degre d differentially homogeneous polynomials in n variables is of dimension n^d. We will also discuss some geometric implications of this result.

The first positive result towards the conjecture was obtained by Reinhart in [2], where he settled the case $n = 2$. The strategy followed by Reinhart was, in essence, very computational. Roughly speaking, he exhibited a candidate for the basis, and described an inductive procedure justifying that every differentially homogeneous polynomial could be expressed as a linear combination of elements in the basis. The inner complexity of this strategy made it difficult to adapt in higher dimensions.

Our strategy takes advantage of a natural action of the general linear group on the space of differentially homogeneous polynomials. Representation theory then allows to reduce drastically the complexity of the problem, making it, somehow, tractable.

Keywords
Differentially homogeneous polynomials, Representation theory.

References
[1] A. ETESSE, On the Schmidt-Kolchin conjecture on differentially homogeneous polynomials. Applications to (twisted) jet differentials on projective spaces. *arXiv preprint, 2023*
[2] G.M. REINHART, The Schmidt-Kolchin conjecture. *Journal of Symboloc Computation* **28**(4-5), 611–631 (1999).

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session on *"Computational Differential and Difference Algebra and its Applications"*

Specializations of normal forms in differential Galois theory

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

Let C be an algebraically closed field of characteristic zero and let $G(C)$ be one of the classical group of Lie type A_l, B_l, C_l, D_l or G_2 (here $l = 2$). Moreover, let $C\{\boldsymbol{v}\}$ be the differential polynomial ring in l differential indeterminates $\boldsymbol{v} = (v_1, \ldots, v_l)$ over C and denote by $C\langle \boldsymbol{v}\rangle$ its field of fractions. In [7,8] we introduced the construction of a general Picard-Vessiot extension $\mathcal{E}$ of a differential field $\mathcal{F}$ of differential transcendental degree l over C having $G(C)$ as its differential Galois group. This extension can be seen as an analogue to the well-known general extension in classical Galois theory whose Galois group is the symmetric group and is defined by the general polynomial equation with coefficients the elementary symmetric polynomials. The field $\mathcal{E}$ in our construction is a Liouvillian extension of the differential field $C\langle \boldsymbol{v}\rangle$ with differential Galois group a Borel group B of G. It is defined by the matrix $A_{\mathrm{Liou}}(\boldsymbol{v})$ in the Lie algebra of the Borel group, which is the sum of the basis elements of the root spaces belonging to the positive simple roots together with a parametrization of the Cartan subalgebra by the indeterminates $\boldsymbol{v}$. For its fundamental solution matrix $b \in B(\mathcal{E})$ and the longest Wey group element $\overline{w}$, we found a matrix u in the maximal unipotent subgroup of G with entries in $C\{\boldsymbol{v}\}$ such that the logarithmic derivative of $Y = u\overline{w}b$ is a specific matrix in the Lie algebra of G which was introduced in [7]. To obtain the base field $\mathcal{F} \subset C\langle \boldsymbol{v}\rangle$ we define a group action of $G(C)$ on $\mathcal{E}$ by right multiplication on Y. The field $\mathcal{F}$ is then the differential fixed field under this action. It is differentially generated over C by Lie rank many differential invariants

$$\boldsymbol{s}(\boldsymbol{v}) = (s_1(\boldsymbol{v}), \ldots, s_l(\boldsymbol{v})) \in C\{\boldsymbol{v}\}^l$$

which are differentially algebraically independent over C. We call the defining matrix differential equation

$$\boldsymbol{y}' = A_G(\boldsymbol{s}(\boldsymbol{v}))\boldsymbol{y}$$

for the general extension $\mathcal{E}$ of $\mathcal{F} = C\langle \boldsymbol{s}\rangle$ the normal form for G (see [6] for the genericity of $A_G(\boldsymbol{s}(\boldsymbol{v}))$).

Let $C(z)$ be the rational function field in the indeterminate z with standard derivation $\frac{d}{dz}$. In this talk we consider specializations

$$\sigma : C(z)\{\boldsymbol{s}(\boldsymbol{v})\} \to C(z), \quad \boldsymbol{s}(\boldsymbol{v}) \mapsto \boldsymbol{f} = (f_1, \ldots, f_l)$$

of the differential invariants $\boldsymbol{s}(\boldsymbol{v})$ to l rational functions $\boldsymbol{f} = (f_1, \dots, f_l)$. We are going to analyse the Picard-Vessiot extension $\overline{\mathcal{E}}$ of $C(z)$ defined by the specialized equation

$$\boldsymbol{y}' = A_G(\sigma(\boldsymbol{s}(\boldsymbol{v})))\boldsymbol{y}$$

and its differential Galois group $\overline{G} \subseteq G$. To this end we design an algorithm to determine the smallest standard parabolic subgroup P (with respect to inclusion of subsets of simple roots) containing a conjugate of $\overline{G}$. This implies for the Levi decompositions $P = R_u(P) \rtimes L(P)$ and $\overline{G} = R_u(\overline{G}) \rtimes L(\overline{G})$ that $R_u(\overline{G}) \subseteq R_u(P)$ and $L(\overline{G}) \subseteq L(P)$. We develop a further algorithm which computes a maximal differential ideal $I \subset C\{\boldsymbol{v}\}$ containing the differential ideal

$$\langle s_1(\boldsymbol{v}) - f_1,\ \dots,\ s_l(\boldsymbol{v}) - f_l \rangle \subset C\{\boldsymbol{v}\}.$$

The field $\overline{\mathcal{E}}$ will then be a Liouvillian extension of the field of fractions of the quotient $C(z)\{\boldsymbol{v}\}/I$ defined by $A_{\mathrm{Liou}}(\overline{\boldsymbol{v}})$ where $\overline{\boldsymbol{v}}$ are the images of $\boldsymbol{v}$ under the canonical projection. The problem of computing the differential Galois group of an arbitrary differential equation is theoretically solved (see [5] and [4,9,1], [2,3]), but until today there is no efficient implementation of such an algorithm. We hope to contribute with this ongoing project to make the algorithms more efficient at least in the special case of a specialization of a normal form matrix for a classical group.

Keywords
Differential Galois theory, normal forms, computational differential Galois theory

References

[1] E. AMZALLAG, A. MINCHENKO AND G. POGUDIN, *Degree bound for toric envelope of a linear algebraic group*. Mathematics of Computation, Volume 91, Issue 335, ISSN 1088-6842, published by the American Mathematical Society, Providence, Rhode Island.
[2] E. COMPOINT AND M.F. SINGER, *Computing Galois Groups of Completely Reducible Differential Equations*. J. Symbolic Computation (1999) 28, 473–494, ISSN 0747-7171, https://doi.org/10.1006/jsco.1999.0311.
[3] T. DREYFUS AND J.A. WEIL, *Computing the Lie algebra of the differential Galois group: The reducible case*. Journal of Symbolic Computation, Volume 112, 2022, Pages 122-163, ISSN 0747-7171, DOI: https://doi.org/10.1016/j.jsc.2022.01.006.
[4] R. FENG, *Hrushovski's algorithm for computing the Galois group of a linear differential equation*. Advances in Applied Mathematics, Volume 65, 2015, Pages 1-37, ISSN 0196-8858, DOI: https://doi.org/10.1016/j.aam.2015.01.001.
[5] E. HRUSHOVSKI, *Computing the Galois group of a linear differential equation*. Banach Center Publications, 58, 97-138, 2002.
[6] D. ROBERTZ AND M. SEISS (2023), *Normal forms in differential Galois theory for the classical groups*. Communications in Algebra, 51:4, 1492-1516,
DOI: 10.1080/00927872.2022.2137520.
[7] M. SEISS, Root Parametrized Differential Equations for the Classical Groups.
arXiv:1609.05535.
[8] M. SEISS, On the Generic Inverse Problem for the Classical Groups. arXiv:2008.12081.
[9] M. SUN (2019), *A new bound on Hrushovski's algorithm for computing the Galois group of a linear differential equation*. Communications in Algebra, 47:9, 3553-3566,
DOI: 10.1080/00927872.2019.1567750.

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session on *"Computational Difference and Differential Algebra and its Applications"*

A classification of first order differential equations

***V. Ravi Srinivasan**, Partha Kumbhakar, Ursashi Roy* [ravisri@iisermohali.ac.in]

Department of Mathematical Sciences, IISER Mohali, Punjab, India

Let k be a differential field of characteristic zero with an algebraically closed field of constants C. In this talk, we initiate a study of first order nonlinear differential equations $f(y, y') = 0$, where f is an irreducible polynomial in two variables, using the theory of strongly normal extensions. We prove that if $f(y, y') = 0$ has a nonalgebraic solution in a differential field extension E of k that can be resolved into a tower of differential fields

$$k = E_0 \subset E_1 \subset \cdots \subset E_{n-1} \subset E,$$

where each E_i is a strongly normal extension of E_{i-1} then every nonalgebraic solutions must be an algebraic function of a solution of some Riccati differential equation or a Weierstrass differential equation defined over an algebraic closure of k. We also prove various results concerning the algebraic dependence of nonalgebraic solutions of a first order differential equation. We will also explain the connections between our work and the recent works by Noordman et al. and Freitag et al on this topic.

Keywords
Strongly normal extensions, Riccati differential equation, Weierstrass differential equation

References

[1] MARC PAUL NOORDMAN; MARIUS VAN DER PUT; JAAP TOP, *Autonomous First Order Differential Equations*. Trans. Amer. Math. Soc. 375 , 1653-1670 (2022).
[2] JAMES FREITAG, RÉMI JAOUI, RAHIM MOOSA , *When any three solutions are independent*. Invent.Math. 230 (3), 1-17 (2022).
[3] PARTHA KUMBHAKAR, URSASHI ROY, V. RAVI SRINIVASAN, *A Classification of First Order Differential Equations*. http://arxiv.org/abs/2302.07083.

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session on *"Computational Difference and Differential Algebra and its Applications"*

Local integrability of polynomial vector fields

Valery G. Romanovski[1,2] [valerij.romanovskij@um.si]

[1] Faculty of Electrical Engineering and Computer Science and Faculty of Natural Science and Mathematics, University of Maribor, Maribor, Slovenia
[2] Center for Applied Mathematics and Theoretical Physics, University of Maribor, Maribor, Slovenia

We discuss the problem of local integrability of polynomial vector fields in a neighborhood of a resonant singular point. The main attention is paid to the case of planar vector fields with $1 : -1$ resonant singular points, that is, vector fields of the form

$$\dot{x} = x + P(x, y), \qquad \dot{y} = -y + Q(x, y), \tag{1}$$

where P and Q are polynomials without constant and linear terms. An efficient method to compute the necessary conditions for existence in a neighborhood of the origin of (1) of an analytic first integral of the form

$$\Psi(x, y) = xy + \sum_{k+m>2} \psi_{km} x^k y^k,$$

is presented. It is based on a specific grading of the formal power series module and reducing to a difference equation. A few mechanisms of integrability are described. A connection to the local 16th Hilbert problem is mentioned.

Keywords
Center problem, First Integral, Limit cycle

References

[1] V. G. ROMANOVSKI AND D. S. SHAFER, *The Center and Cyclicity Problems: A Computational Algebra Approach*. Birkhäuser, Boston, 2009.
[2] T. PETEK AND V. G. ROMANOVSKI, Computation of Normal Forms for Systems with Many Parameters, arXiv:2305.01739, 2023.

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session on *“Algebraic Geometry from an Algorithmic Point of View”*

Jet schemes of Pfaffian ideals

Emanuela De Negri[1], ***Enrico Sbarra*** [2] `[denegri@dima.unige.it]`

[1] Mathematics Department, University of Genova, Genova, Italy
[2] Mathematics Department, University of Pisa, Italy

Jet schemes and arc spaces received quite a lot of attention by researchers after their introduction, due to J. Nash, and established their importance as an object of study in M. Kontsevich's motivic integration theory. Several results point out that jet schemes carry a rich amount of geometrical information about the original object they stem from, whereas, from an algebraic point of view, little is know about them.

In this talk we consider the ideal I_{2r} generated by the pfaffians of size $2r$ in an $n \times n$ generic skew-symmetric matrix and, inspired by [2], we study algebraic properties of the corresponding k-th jet schemes ideal $I_r^{n,k}$. In particular we determine under which conditions the corresponding jet scheme varieties are irreducible. Moreover in the case $n = 2r$ we prove that for every k the natural generators of $I_r^{n,k}$ are a Gröbner basis, and that $I_r^{n,k}$ defines a Cohen Macaulay domain of multiplicity r^k. Conjectures and open questions will be stated.

Keywords
Determinantal ideal, Jet schemes ideals

References

[1] E. De Negri, E. Sbarra, On jet schemes of pfaffian ideals. *Collectanea Mathematica* **70** (2019), 479–491.
[2] T. Košir, B.A Sethuraman, Determinantal varieties over truncated polynomial rings. *J. Pure Appl. Algebra* **195** (2005), 75–95.

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session on *"Algebraic Geometry from an Algorithmic Point of View"*

Binary curves of genera four and five

Dušan Dragutinović[1] [d.dragutinovic@uu.nl]

[1] Mathematical Institute, Utrecht University, Utrecht, Netherlands

In [1], Xarles makes a census of all genus-4 curves defined over $\mathbb{F}_2$, the field with two elements, up to isomorphism. Inspired by that, we compute in [2] the isomorphism classes of genus-5 curves over $\mathbb{F}_2$, which can be either hyperelliptic, trigonal, or whose canonical model is a complete intersection of three quadrics in $\mathbb{P}^4$. In addition, for each curve, we determine its automorphism group over $\mathbb{F}_2$.
While some analogous ideas to Xarles's can be used for curves of the first two types, the third type of curves and their automorphism groups need special attention. Our algorithm for computing the isomorphism classes of non-hyperelliptic, non-trigonal curves is based on the exhaustion of eligible triples of quadratic polynomials in five variables and uses some elementary ways of expressing when two such triples can define isomorphic curves and what those isomorphisms can be. Namely, being canonical, the isomorphism among them is induced by an element of $\mathrm{PGL}_5(\mathbb{F}_2)$, so that we should find a subset of a reasonable size of the set of all such triples, and for every two triples, a subset of $\mathrm{PGL}_5(\mathbb{F}_2)$ whose elements can establish a potential isomorphism among the curves they define. As an outcome of the SAGEMATH implementation available at [3] and the data we obtain, we compute the weighted number of such curves and show the existence of any eligible Newton polygon of height 10 for them.
Furthermore, we analyze in [4] the data provided by Xarles and the data of isogeny classes of abelian fourfolds over $\mathbb{F}_2$ from [5]. Essentially, by comparing them, we show that not all the supersingular principally polarized abelian fourfolds over $\mathbb{F}_2$ are Jacobians and use that to determine the dimensions of the Newton polygon strata inside the 2-rank zero locus of the moduli space of genus-4 curves in characteristic two.

Keywords
Curves, automorphisms, finite fields, data, geometry

References
[1] X. XARLES, *A census of all genus 4 curves over the field with 2 elements*. arXiv:2007.07822.
[2] D. DRAGUTINOVIĆ, *Computing binary curves of genus five*. arXiv:2202.07809. (Submitted.)
[3] `https://github.com/DusanDragutinovic/Non-hyp-non-trig-genus-5-over-F_2`
[4] D. DRAGUTINOVIĆ, *Supersingular curves of genus four in characteristic two*. arxiv:2301.12897. (Submitted.)
[5] THE LMFDB COLLABORATION, *The L-functions and modular forms database*. http://www.lmfdb.org.

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session on *"Algebraic Geometry from an Algorithmic Point of View"*

Free Resolutions and Generalized Hamming Weights of binary linear codes

Ignacio García-Marco[1] [1], ***Irene Márquez-Corbella*** [1], ***Edgar Martínez-Moro***[2] ***and Yuriko Pitones***[3] [iggarcia@ull.edu.es]

[1] Instituto de Matemáticas y Aplicaciones de la Universidad de La Laguna (IMAULL) and Departamento de Matemáticas, Estadística e I.O., Universidad de La Laguna, Tenerife, Spain
[2] Institute of Mathematics, University of Valladolid, Castilla, Spain
[3] Universidad Autónoma Metropolitana, México

Let $\mathbb{F}_q$ be a finite field with q elements. Given a k-dimensional linear code $\mathcal{C} \subseteq \mathbb{F}_q^n$, the r-th Hamming weight of $\mathcal{C}$ is the minimum of the support sizes of all the r-dimensional subcodes of $\mathcal{C}$, for $r \in \{1, \ldots, k\}$. The study of the Generalized Hamming Weights (GHWs) has been motivated by several applications in cryptography [4]. For instance, these weights characterize the code performance on a wire-tap channel. There are few families of codes for which it is known the complete generalized weight hierarchy as for example: first-order Reed-Muller codes, binary Reed-Muller codes or Hamming code and its dual.

In their seminal paper [3], Johnsen and Verdure showed how the GHWs of a linear code can be computed by means of a minimal graded free resolution of the monomial ideal associated to the set of codewords of minimal support of the code. This paper produced a great avenue of research. One of the main drawbacks of Johnsen and Verdure's approach is that the set of codewords of minimal support is usually a huge set and it is expensive to compute. Hence, it would be desirable to find smaller structures providing information on the GHWs.

In the present work, we consider binary codes and we explore what information on the GHWs can be extracted from the so-called *test sets*, intrduced by Borges-Quitana et al. in [1]. These sets are constructed from the support of the binomials in a Gröbner basis of an ideal associated to the code with respect to a graded monomial ordering. In [1] the authors prove that one can extract a big amount of relevant information of the code from them. In particular, they can be used for decoding and for computing the minimum distance of the code (and, thus, the first GHW). In this work we show how one can also compute the second GHW and provide upper bounds on the whole hierarchy of GHWs of a binary linear code from a test set. We finish by presenting several conjectures and open problems concerning the computation of the GHWs.

The results of this talk are included in [2].

[1]The author is partially supported by "Plan de incentivación de la actividad investigadora 2023" of Universidad de La Laguna and by the grant PID2019-105896GB-I00 funded by MCIN/AEI/10.13039/501100011033

Keywords
binary linear code, generalized Hamming weight, binomial ideal, minimal graded free resolution

References

[1] M. BORGES-QUINTANA; M. A. BORGES-TRENARD; P. FITZPATRICK; E. MARTÍNEZ-MORO, Gröbner bases and combinatorics for binary codes. *Appl. Algebra Engrg. Comm. Comput.* **19**(5), 393–411 (2008).

[2] I. GARCÍA-MARCO; I. MÁRQUEZ-CORBELLA; E. MARTÍNEZ-MORO; Y. PITONES, Free Resolutions and Generalized Hamming Weights of Binary Linear Codes. *Mathematics* **10**, 2079 (2022).

[3] T. JOHNSEN; H. VERDURE, Hamming weights and Betti numbers of Stanley-Reisner rings associated to matroids. *Appl. Algebra Engrg. Comm. Comput.* **24**(1), 73–93 (2013).

[4] V.K. WEI Generalized Hamming weights for linear codes. *IEEE Trans. Inf. Theory* **37**, 1412–1418, (1991).

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session on *"Algebraic Geometry from an Algorithmic Point of View"*

Infinite free resolutions induced by Pommaret-like bases over Clements–Lindström rings

Amir Hashemi[1,2]***, <u>Matthias Orth</u>***[3]***, Werner M. Seiler***[3] [morth@mathematik.uni-kassel.de]

[1] Department of Mathematical Sciences, Isfahan University of Technology, Isfahan 84156-83111, Iran
[2] School of Mathematics, Institute for Research in Fundamental Sciences (IPM), Tehran, 19395-5746, Iran
[3] Institut für Mathematik, Universität Kassel, Heinrich-Plett-Str. 40, 34132 Kassel, Germany

Free resolutions are an important tool in algebraic geometry for the analysis of modules over polynomial rings and their quotient rings. Minimal free resolutions are unique up to isomorphism and contain homological invariants. It is known that Pommaret bases of ideals in the polynomial ring induce finite free resolutions and that the Castelnuovo-Mumford regularity and projective dimension can be easily obtained already from the Pommaret basis. In this talk, we will introduce the concept of Pommaret-like bases and how these bases can be used for the analysis of infinite free resolutions over Clements–Lindström rings.

We work over the quotient rings of a polynomial ring $\mathcal{R} = K[x_1, \ldots, x_n]$ over a field K. Thus given a homogeneous ideal $\mathcal{I} \subseteq \mathcal{R}$, we make the computations in the ring $\mathcal{R}/\mathcal{I}$. A special case for $\mathcal{I} = \{0\}$ is the ring $\mathcal{R}$ itself. We write $\mathcal{T}$ for the set of all terms $x^\mu = x_1^{\mu_1} \cdots x_n^{\mu_n} \in \mathcal{R}$ with $\mu = (\mu_1, \ldots, \mu_n)$.

We construct free resolutions of homogeneous ideals $\mathcal{J} \trianglelefteq \mathcal{R}/\mathcal{I}$. A free resolution $\mathbf{F}$ of $\mathcal{J}$ is given by finitely generated free $\mathcal{R}/\mathcal{I}$-modules $F_0, F_1, \ldots$ and homogeneous $\mathcal{R}/\mathcal{I}$-linear maps $\delta_0, \delta_1, \delta_2, \ldots$ as in the following diagram:

$$\mathbf{F}: \quad \cdots \xrightarrow{\delta_{m+2}} F_{m+1} \xrightarrow{\delta_{m+1}} F_m \xrightarrow{\delta_m} F_{m-1} \xrightarrow{\delta_{m-1}} \cdots \xrightarrow{\delta_2} F_1 \xrightarrow{\delta_1} F_0 \xrightarrow{\delta_0} \mathcal{J} \to 0,$$

with $\operatorname{im}(\delta_0) = \mathcal{J}$ and $\operatorname{im}(\delta_{m+1}) = \ker(\delta_m)$ for all $m \geq 0$. The collection $\{\delta_m\}_{m \geq 0}$ of maps is called the *differential* of the resolution. Leaving aside degree shifts, we can write $F_m = (\mathcal{R}/\mathcal{I})^{r_m}$ for $m \geq 0$. Each δ_m is described by the images $\delta(\vec{e}_i)$, $i \in \{1, \ldots, r_m\}$; equivalently, δ_m is represented by a matrix $D_m \in (\mathcal{R}/\mathcal{I})^{r_{m-1} \times r_m}$, whose i-th column is $\delta_m(\vec{e}_i)$. Moreover, $D_m \cdot D_{m+1} = 0$ for all m. The set $G := \{\delta_0(\vec{e}_1), \ldots, \delta_0(\vec{e}_{r_0})\}$ is a homogeneous generating set of $\mathcal{J}$ and the columns of D_1 are a homogeneous generating set G_1 of the first syzygy module $\operatorname{Syz}(G)$. Generally, the set G_m of columns of D_m is a homogeneous generating set of the iterated syzygy module $\operatorname{Syz}^m(G)$. For a more detailed introduction to infinite graded free resolutions and an overview of associated research questions, see [7].

Pommaret-like bases are an adapted form of Pommaret bases, which are types of involutive bases. Involutive bases are Gröbner bases with special combinatorial properties introduced by Zharkov and Blinkov [10] and further studied by Gerdt and Blinkov [4]. An overview of theory, algorithms and applications can be found in [9]. They arise via a restriction of the usual divisibility relation of terms to an involutive division.

We shortly describe the Pommaret division. The *class* of a term $1 \neq x^{\mu} \in \mathcal{T}$ with $\mu = (\mu_1, \ldots, \mu_n)$ is defined as the index $\operatorname{cls}(x^{\mu}) = \min\{i \mid \mu_i \neq 0\}$. A variable x_i is Pommaret multiplicative for x^{μ}, if $i \leq \operatorname{cls}(x^{\mu})$. Not every monomial ideal has a finite Pommaret basis; those that do are called *quasi-stable*. A polynomial ideal $\mathcal{I}$ is in *quasi-stable position*, if its leading ideal with respect to a term-order is quasi-stable.

The Pommaret-like division is based on the Janet-like division introduced by Gerdt and Blinkov [5]. Let $U \subset \mathcal{T}$ be a finite set of terms. For any term $u \in U$ and any index $1 \leq i \leq n$, a *non-multiplicative power* of u for the *Janet-like division* at the variable x_i exists, if there is a term $v \in U$ with $\deg_j(v) = \deg_j(u)$ for all $i < j \leq n$ and $\deg_i(v) > \deg_i(u)$. The non-multiplicative power is then given by $x_i^{h_i(u,U)}$, where $h_i(u,U)$ is the minimal positive value of $\deg_i(v) - \deg_i(u)$ as v ranges over all terms in U with the properties just mentioned. The set of all non-multiplicative powers of $u \in U$ is denoted by $\operatorname{NMP}(u, U)$.

Definition 1. The *Pommaret-like division* P assigns to each term $t \in \mathcal{T}$ contained in a finite set of terms $U \subset \mathcal{T}$, the following non-multiplicative powers: (1) All Janet-like non-multiplicative powers $x_a^{p_a}$ with $a > \operatorname{cls}(t)$. (2) The variables x_b with $b > \operatorname{cls}(t)$ for which there exists no Janet-like non-multiplicative power.

For a given monomial ideal, a finite Pommaret-like basis exists if and only if the ideal is quasi-stable. This basis is in general smaller than the Pommaret basis of the same ideal. We extend the Pommaret-like division also to ideals in monomial quotient rings. For a quasi-stable ideal $\mathcal{I}$ and a monomial ideal $\mathcal{J} \subseteq \mathcal{R}/\mathcal{I}$, a Pommaret-like basis for $\mathcal{J}$ exists if and only if $\mathcal{J}$ is the image of a quasi-stable ideal in $\mathcal{R}$. We write $P_{\mathcal{I}}$ for the Pommaret-like division in $\mathcal{R}/\mathcal{I}$. To emphasize that we are working in a quotient ring, we speak of a *relative Pommaret-like basis*. In [6], the syzygies of relative Pommaret bases were analysed, using a suitable module term ordering and applying a construction due to Schreyer [8]. We generalize this to relative Pommaret-like bases in quotient rings $\mathcal{R}/\mathcal{I}$ defined by an irreducible quasi-stable monomial ideal $\mathcal{I}$. By iteration, we obtain a free resolution together with Pommaret-like bases for the first and all higher syzygy modules. These Pommaret-like bases are reduced Gröbner bases.

Adapting the definitions due to [1] to our conventions on variable orderings, we say that an irreducible, non-zero monomial ideal $\mathcal{I} \trianglelefteq \mathcal{R}$ is *Clements-Lindström*, if its minimal generating set is of the form $\{x_i^{a_i}, x_{i+1}^{a_{i+1}}, \ldots, x_n^{a_n}\}$ with $2 \leq a_n \leq a_{n-1} \leq \cdots \leq a_{i+1} \leq a_i$. We call $\mathcal{R}/\mathcal{I}$ a *Clements-Lindström ring*.

Theorem 2. *Let $\mathcal{I} \trianglelefteq \mathcal{R}$ be a Clements-Lindström ideal and let $\mathcal{J} \supset \mathcal{I}$ be a monomial ideal generated by the minimal Pommaret-like basis $H \subset (\mathcal{J} \setminus \mathcal{I}) \cap \mathcal{T}$ relative to $\mathcal{I}$. Assume that H is also the minimal monomial generating set of $\mathcal{J}$ relative to $\mathcal{I}$ and that for each $t \in H$ and $x_a^{p_a} \in \operatorname{NMP}_{P_{\mathcal{I}}}(t, H)$, the unique $P_{\mathcal{I}}$-divisor $s \in H$ of $t \cdot x_a^{p_a}$ fulfils $\operatorname{cls}(s) > \operatorname{cls}(t)$. Then the free resolution of $\mathcal{J}$ over $\mathcal{R}/\mathcal{I}$ induced by the basis H is the minimal free resolution of $\mathcal{J}$ over $\mathcal{R}/\mathcal{I}$.*

Let $\mathcal{J} \supseteq \mathcal{I}$ be any homogeneous polynomial ideal in quasi-stable position relative to $\mathcal{I}$ with respect to the degrevlex term ordering. Moreover, assume that the minimal Pommaret-like basis of $\mathcal{J}$ relative to $\mathcal{I}$ is a minimal homogeneous generating set and that the resolution induced by this Pommaret-like basis over the ring $\mathcal{R}/\mathcal{I}$ is minimal. We construct a basis for the bigraded free $\mathcal{R}/\mathcal{I}$-module supporting the resolution, only using the Pommaret-like basis of the leading ideal of $\mathcal{J}$ relative to $\mathcal{I}$, and also give a formula for the Poincaré series of the resolution using only these data. Note that the Poincaré series encodes the bigraded Betti numbers of the resolution.

Consider a Pommaret-like basis H relative to $\mathcal{I} = \langle x_k^{h_k}, x_{k+1}^{h_{k+1}} \ldots, x_n^{h_n} \rangle$. We write $\operatorname{supp}(\mathcal{I}) := \{x_k, x_{k+1}, \ldots, x_n\}$. The induced free resolution is supported on free $\mathcal{R}/\mathcal{I}$-modules. The first free $\mathcal{R}/\mathcal{I}$-module M_0 has a basis that we enumerate as $\{\vec{e}_\alpha \mid h_\alpha \in H\}$. The ideals $\mathcal{J}_\alpha = \langle x_i^{d_i} \mid x_i^{d_i} \cdot \vec{e}_\alpha \in \operatorname{lt}(\operatorname{Syz}(H)) \rangle$ are irreducible and we write $\operatorname{supp}(\mathcal{J}_\alpha)$ for the set of variables appearing in their respective generating sets. For the r-th module F_r in the resolution, we obtain a basis made of elements of the form $\vec{e}_{\alpha,x^\mu}$, where x^μ is a term of degree r with $\operatorname{cls}(x^\mu) \geq \operatorname{cls}(t_\alpha)$. Moreover, x^μ is supported on $\operatorname{supp}(\mathcal{J}_\alpha)$, and its projection onto $\operatorname{supp}(\mathcal{J}_\alpha) \setminus \operatorname{supp}(\mathcal{I})$ is square-free.

We apply our results to square-free Borel ideals and show that the minimal free resolution for such ideals found in [3] is a Pommaret-like induced resolution. Finally, we note that if we apply our construction to Pommaret-like bases in the polynomial ring $\mathcal{R}$, we obtain for some classes of quasi-stable ideals an explicit formula for the differential of the Pommaret-like induced resolution. This construction generalizes, in particular, resolution formulas for stable and quasi-stable monomial ideals due to Eliahou and Kervaire [2] and Seiler [9], respectively.

Keywords
Polynomial rings, monomial quotient rings, Gröbner bases, syzygy modules, free resolutions

References

[1] G.F. Clements, B. Lindström, A generalization of a combinatorial theorem of Macaulay. *J. Comb. Theory* **7**, 230–238 (1969).
[2] S. Eliahou, M. Kervaire, Minimal resolutions of some monomial ideals. *J. Algebra* **129**(1), 1–25 (1990).
[3] V. Gasharov, S. Murai, I. Peeva, Applications of mapping cones over Clements-Lindström rings. *J. Algebra* **325**(1), 34–55 (2011).
[4] V.P. Gerdt, Y.A. Blinkov, Involutive bases of polynomial ideals. *Math. Comput. Simul.* **45**(5-6), 519–541 (1998).
[5] V.P. Gerdt, Y.A. Blinkov, Janet-like monomial division. In *Computer Algebra in Scientific Computing, CASC 2005*, 174–183. Springer, 2005.
[6] A. Hashemi, M. Orth, W.M. Seiler, Relative Gröbner and involutive bases for ideals in quotient rings. *Math. Comput. Sci.* **15**(3), 453–482 (2021).
[7] J. McCullough, I. Peeva, Infinite graded free resolutions. In *Commutative algebra and noncommutative algebraic geometry. Volume I: Expository articles*, 215–257. Cambridge: Cambridge University Press, 2015.
[8] F.O. Schreyer, Die Berechnung von Syzygien mit dem verallgemeinerten Weierstrass-'schen Divisionssatz. Master's thesis, University of Hamburg, Germany, 1980.
[9] W.M. Seiler, Involution. The formal theory of differential equations and its applications in computer algebra. Springer, Berlin, 2010.
[10] A.Y. Zharkov, Y.A. Blinkov, Involution approach to investigating polynomial systems. *Math. Comput. Simul.* **42**(4), 323–332 (1996).

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session on *"Algebraic Geometry from an Algorithmic Point of View"*

The m-ovoids of $\mathcal{W}(5,2)$ and their generalizations

Michela Ceria[1]***, Francesco Pavese***[1] `[michela.ceria@poliba.it]`

[1] DMMM, Politecnico di Bari, Bari, Italy

Consider the projective space $PG(2n+1,q)$ over the finite field $\mathbb{F}_q$. Let V be the associated vector space. The symplectic polar space $\mathcal{W}(2n+1,q)$ is given by all totally isotropic subspaces of V with respect to a non-degenerate alternating form of V. They are the subspaces that are contained in their orthogonal complement with respect to such form.

The projective subspaces of maximal dimension that are contained in $\mathcal{W}(2n+1,q)$ are the *generators* of $\mathcal{W}(2n+1,q)$ and, given them, we can define the main objects of this talk: the m*-ovoids*. A m-ovoid of $\mathcal{W}(2n+1,q)$ is a set $\mathcal{O}$ of its points such that all generators meet $\mathcal{O}$ in *exactly* m points.

Point sets of this kind are 2-*character sets*, namely each hyperplane has only two possible intersections with these points. This makes the sets *equivalent* to projective codes with two weights and also such sets give rise to strongly regular Cayley graphs.

The study of m-ovoids has a long history, starting from B. Segre [1], Tits [2] and Suzuki [3]. Thas [4], in 1981, proved that $\mathcal{W}(2n+1,q)$ has an -ovoid (that is, m-ovoid with $m=1$) if and only if $n=1$ and q is an even prime power, while Shult and Thas [5] defined for the first time m-ovoids in 1994 and then many constructions followed, for example via field reduction [6] or strongly regular graphs [7].

In this talk we concentrate on the even case showing the existence of an m-ovoid of $\mathcal{W}(2n+1,q)$ with $m=\frac{q^n-1}{q-1}$, given by an elliptic quadric of $PG(2n+1,q)$ not polarizing to the symplectic polar space.

Moreover, we find out a new class of $(q+1)-$ovoids of $\mathcal{W}(5,q)$ and a classification if $q=2$.

The talk refers to the paper [8], joint work with Francesco Pavese (Politecnico di Bari).

Keywords
m-ovoids, 2-character sets, symplectic polar space

References

[1] B. SEGRE On complete caps and ovaloids in three-dimensional Galois spaces of charac-

teristic two, *Acta Arithmetica* **V** (1959).
[2] J. TITS Ovoïdes et Groupes de Suzuki, *Archiv der Mathematik* (1962)
[3] M. SUZUKI A new type of simple groups of finite order. *Proc. Nat. Acad. Sci. U.S.A.* **46**, 868–870 (1960).
[4] J.A. THAS, Ovoids and spreads of finite classical polar spaces, *Geom. Dedic.* **10** 135–143 (1981).
[5] E.E. SHULT, J.A. THAS, m-systems of polar spaces, *J. Comb. Theory, Ser. A* **68** 184–204 (1994).
[6] S. KELLY, Constructions of intriguing sets of polar spaces from field reduction and derivation, *Des. Codes Cryptogr.* **43** 1–8 (2007).
[7] T. FENG, Y. WANG, Q. XIANG, On m-ovoids of symplectic polar spaces, *J. Comb. Theory, Ser. A* **175** 105279 (2020).
[8] M. CERIA, F. PAVESE, The m-ovoids of $\mathcal{W}(5, 2)$ and their generalizations. *Finite Fields and Their Applications* **84** (2022).

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session on *"Algebraic Geometry from an Algorithmic Point of View"*

Degroebnerization for data modelling problems

Teo Mora[1], ***Michela Ceria***[2], ***Andrea Visconti*** [3] [theofmora@gmail.com]

[1]DIMA- Università di Genova, Genova, Italy
[2] DMMM, Polytechnic University of Bari, Bari, Italy
[3] Dipartimento di Informatica "Giovanni degli Antoni", Università di Milano, Milano, Italy

Gröbner bases's theory plays an important role in Computer Algebra and many applications have been solved by considering them as a preprocessing, and saying "if we have the Gröbner basis, then the problem is easily solved". This is undoubtedly true, but it does not take into account that *finding a Gröbner basis is not always an easy task*. The computation can become computationally hard and there are cases in which it is even infeasible.

Luckily, there are practical problems for which Gröbner bases are not the only way to get a solution, and this allows us to switch to a new paradigm: *Degröbnerization* [1].

In Degröbnerization we completely change perspective in the algebraic representation of our problems, substituting the prior representation, based on *polynomial ideals* to a representation given by *quotient algebras*, expressed via a vector-space basis and multiplication (Auzinger-Stetter) matrices.

This has the immediate advantage to open to new operational methods, that base on linear algebra and combinatorics and that can provide efficient solutions to (some of) the aforementioned practical problems. One of them is *data modelling*, that we face in this talk from the point of view of the application to reverse engineering for gene regulatory networks, improving the Computer Algebra method given by Lauenbacher and Stigler [2].

In such context normal forms of polynomials modulo the ideal of some data points is needed. We show that the problem can be faced without even introducing the ideal of points, but only relying on the points themselves.

In particular, only combinatorial methods (such that the use of trees to compare the coordinates of data points, and Bar Codes), evaluations and linear algebra methods (matrix inversion, matrix multiplications) are the tools needed to construct a model and we show abstract computational complexity advantages as well as some implementation details.

Keywords
Degroebnerization, reverse engineering for gene regulatory networks, Bar Codes

References

[1] M. CERIA, S. LUNDQVIST, T. MORA , Degröbnerization: a political manifesto, *Applicable Algebra in Engineering, Communication and Computing*, **33** (6), 675 – 723, (2022).

[2] R. LAUENBACHER, B. STIGLER, A computational algebra approach to the reverse engineering of gene regulatory networks, *Journal of Theoretical Biology*, **229** (4), 523–537, Academic Press (2004).

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session on *"Algebraic Geometry from an Algorithmic Point of View"*

Generalizing Möller algorithm: a flexibility issue

Teo Mora[1]***, Michela Ceria***[2] [theofmora@gmail.com]

[1]DIMA- Università di Genova, Genova, Italy
[2]DMMM, Polytechnic University of Bari, Bari, Italy

The two conferences presented here are part of a series of articles in the context of Degröbnerization [1,4-8], a research topic proposed at the previous ACA [1] and are both devoted to two of the main tools of Degröbnerization:

- Cerlienco–Mureddu Correspondence [9-11] of which in [3] we describe our implementation based on a political change of perspective; we represent the algebraic structure related to a (finite) set of points as a *quotient algebra* expressed via a vector-space and Auzinger–Stetter multiplication matrices [12].
- the original *Möller Algorithm* [13] proceeding by induction on the points[1] of which we presented in ACA2021 [1] and ISSAC'22 [4] a version available for each ideal defined by (non-necessarily commutative) functionals over any *effective ring* claiming that it can use *any* total ordering (not necessarily a semigroup one) for ordering the terms needed to express the wanted vector-space basis.

We recall that classical Möller Algorithm

- ⋄ takes as input a set of functionals ordered in such a way that each initial segment defines a zero-dimensional ideal thus producing a Macaulay chain [17] of such ideal,
- ⋄ which is easily produced for a 0-dimensional ideal of polynomials;
- ⋄ requires at most the evaluation of each such functional to each term needed to express the wanted vector-space basis and
- ⋄ produces for each ideal in the Macaulay chain not only its representation as a *quotient algebra* expressed via a vector-space and Auzinger–Stetter multiplication matrices,
- ⋄ but also triangular and separator polynomials can be derived, as in the original version, as well as the transformation matrix linking them.

[1]differently from *Buchberger-Möller Algorithm* [14-16] which proceeds by induction on terms.

What made us orient our investigation towards a version of the algorithm which at the same time did not require a semigroup ordering and that covers a wide class of algebras was a careful reading of [2], which is a strong supporter of both the application of Gröbnerian technology and Buchberger-Möller Algorithm towards Algebraic Statistics and where we read

- *Another class of statistical models we shall consider are linear models whose vector space basis is formed by polynomials which are not monomials*;
- *Example 7 is not a corner cut*[2] *model. However, it is the most symmetric of the models in the statistical fan. In fact, to destroy symmetry is a feature of Gröbner basis computation, as term orderings intrinsically do not preserve symmetries, which are often preferred in statistical models* .

In this talk, we describe the present version of *Möller Algorithm* and illustrate its greater flexibility both via a finite example where the terms are ordered by an ordering which is not a semigroup one and by giving a symmetric basis of the ideal (Example 7) discussed in [2].

Keywords
Möller algorithm, interpolation, Auzinger–Stetter matrices

References
[1] M. CERIA, S. LUNDQVIST, T. MORA , Degröbnerization: a political manifesto, *Applicable Algebra in Engineering, Communication and Computing*, **33** (6), 675 – 723, (2022).
[2] G. PISTONE, E. RICCOMAGNO, M.P. ROGANTIN Methods in Algebraic Statistics for the Design of Experiments. *In: Pronzato, L., Zhigljavsky, A. (eds) Optimal Design and Related Areas in Optimization and Statistics. Springer Optimization and Its Applications*, **28**, Springer, New York, NY, (2009).
[3] T. MORA, M. CERIA, A. VISCONTI, Degroebnerization for data modelling problems, Abstract for ACA2023
[4] M. CERIA, F. MORA, A Degroebnerization Approach to Algebraic Statistics *Proceedings of the International Symposium on Symbolic and Algebraic Computation, ISSAC, 2022* 419–428.
[5] M. CERIA, S. LUNDQVIST, T. MORA , Degröbnerization and Its Applications: Reverse Engineering of Gene Regulatory Networks, *CEUR Workshop Proceedings of the 6th International Workshop on Satisfiability Checking and Symbolic Computation*, **3273**, 27–30.
[6] T. MORA, `http://www.dima.unige.it/$\sim$morafe/SLIDES/TR8.pdf`, Accessed: 2021-11-22
[7] T. MORA, `http://www.dima.unige.it/$\sim$morafe/SLIDES/SantiagoMacaulay.pdf`, Accessed: 2021-11-22
[8] T. MORA, `http://www.dima.unige.it/$\sim$morafe/SLIDES/BondingUMI.pdf`, Accessed: 2021-11-22
[9] L. CERLIENCO, M. MUREDDU , Algoritmi combinatori per l'interpolazione polinomiale in dimensione ≥ 2, *Publ. I.R.M.A. Strasbourg, 1993, 461/S-24 Actes* 24^e *Séminaire Lotharingien*, 39–76.

[2]Recall that a Monomial Basis of a 0-dimensional ideal of polynomials which is *Hierarchical, i.e.* an order ideal, is called a *Corner Cut* when it is the Gröbner escalier/normal set modulo the Gröbner basis of such ideal w.r.t. a term ordering.

[10] L. CERLIENCO, M. MUREDDU , From algebraic sets to monomial linear bases by means of combinatorial algorithms, *Discrete Math.* **139**, 73–87.
[11] L. CERLIENCO, M. MUREDDU , Multivariate Interpolation and Standard Bases for Macaulay Modules, *J. Algebra* **251**, 686–726, (2002).
[12] W. AUZINGER, H.J. STETTER, An elimination algorithm for the computation of all zeros of a system of multivariate polynomial equations, *Numerical Mathematics Singapore 1988*, 11–30, (1988) Springer
[13] M.G. MARINARI, H.M. MÖLLER, T MORA, Gröbner bases of ideals defined by functionals with an application to ideals of projective points, *Applicable Algebra in Engineering, Communication and Computing* **4** (2), 103–145 (1993)
[14] B. BUCHBERGER, H.M. MÖLLER, The construction of multivariate polynomials with preassigned zeros, *European Computer Algebra Conference*, 24–31, Springer, (1982)
[15] T. MORA, L. ROBBIANO, Points in affine and projective spaces, *Computational Algebraic Geometry and Commutative Algebra, Cortona-91*, **34**, 106–150, (1993) Cambridge University Press
[16] J. ABBOTT, A. BIGATTI, M. KREUZER. L. ROBBIANO, Computing ideals of points, *Journal of Symbolic Computation*, **30**, (4), 341–356, (2000), Elsevier
[17] M.E. ALONSO, M.G. MARINARI, M.T. MORA The Big Mother of All the Dualities, II: Macaulay Bases. *J. AAECC* **17**, 409–451 (2006).

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session on *"Algebraic Geometry from an Algorithmic Point of View"*

On classification of algebraic curves and surfaces, using algorithmic methods

Meirav Amram[1] [meiravt@sce.ac.il]

[1] Mathematics Department, SCE, Israel

The classification of algebraic curves and surfaces in a moduli space is a challenging subject in algebraic geometry. Moduli spaces are spaces that parameterize families of algebraic surfaces. They can be used to study the geometry of algebraic surfaces and to compare different surfaces. Classifying algebraic surfaces and curves is an important task because of the comparison between different objects that we study. The moduli space of curves for example, is a space that parameterizes families of algebraic curves of a fixed genus.

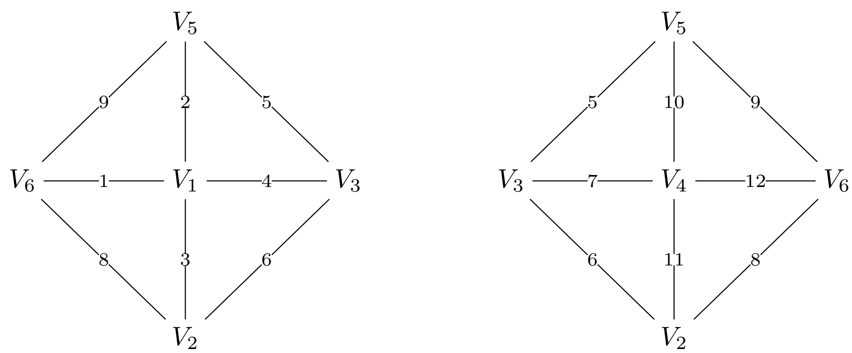
The objects we study and classify can be algebraic curves that are potentially Zariski pairs, and algebraic surfaces with their related degenerations and fundamental groups.

There are methods that can assist in this classification, for example: topological classification, intersection theory, singularities, cohomology, symmetric groups, etc. There are known algorithmic methods as well, and the choice of a method depends on the specific properties of the surface or curve in question and the desired level of detail in the classification.

In the mathematical community, the researchers use the computer programs Magma, Singular, Maple, and so on. These are just a few examples of software packages that can be used for classifying algebraic surfaces and curves. The choice of software depends on the specific needs and preferences of the researcher. In our research we use mostly Magma because we investigate fundamental groups and the Magma is a great tool for this goal. In fact, Magma can simplify presentations of groups in general, and of fundamental groups in particular, by means of generators and relations. Therefore in our work we need to use the output we get from Magma for a manual continuation of simplification, or we can use other programs that we built especially for determination of our fundamental groups.

Except Magma, we use two self-constructing computer programs in our research. In order to adapt the difficulty and length of the calculations to our research needs, we can construct such computer programs that shorten processes and time, and make the results accessible in an accurate and reliable way. The developed computer programs that are mentioned were jointly constructed with Uriel Sinichkin (Tel-Aviv University, Israel). Those programs were implemented in Python.

Before we explain about the two computer programs, we want to give you in the following figure an understanding about the level of complexity of the computations and the multiplicity of singularities. It happens especially when we glue two degeneration or when we consider a non-planar degenerations. In the figure in particular, we can see two planar degenerated pieces that are glued together along four edges, and we get a non-planar degeneration with multiplicity 4 in all singularities.



Now we explain how classification of algebraic curves and surfaces merges with the use of these algorithmic methods in our research. We take an algebraic surface embedded in a projective space and project it with a generic projection onto the projective plane. We get the branch curve and then we are able to calculate G - the fundamental group of its complement. This is done using our first self-constructing computer program. This program gives as output all braids relating to the branch curve and also the presentation of G. We use this output to find a certain quotient of G, which is going to be the fundamental group of the Galois cover of the surface. This latter group is an invariant in the classification of algebraic surfaces, and has a geometric significance because it is equal for all the surfaces in the same connected component in the moduli space. Details about the fundamental groups of Galois cover of an algebraic surface and some interesting examples can be found in our works [1,2,3]. In these recent works, we work with algebraic surfaces with degenerations that have R_k singularities (for any k) [1], and surfaces that have non-planar degenerations, in which singularities with high complexity appear [2,3].

Here are the steps of the work with the softwares: Our first self-constructing software gives us the braids and the presentation of the fundamental group G (applying the van-Kampen Theorem [4]). The fundamental group of the Galois cover is the quotient of G, and this group will be the input given to Magma. We admit that Magma is very helpful at this stage because we give the list of generators and relations of the group as an input, and run the program. Magma simplifies the presentation and eliminates a few generators from the presentation. After we have the output, we cannot always use the traditional methods of simplification of groups (for example, manual simplification and basic group theory), and we need a much more sophisticated computer program that helps us to determine the group. Therefore, with our second self-constructing computer program we can define an isomorphism between our group and some Coxeter quotient. Thanks to our familiarity with Coxeter groups (or perhaps also Artin groups, depending on the level of complexity of the surface we investigate), it is easier to deal with the calculations. The presentation is better explained and the shape of the groups is better understood. This software was constructed based on the knowledge we have from work [5].

As for algebraic curves, we can use the first software that we constructed in order to produce braids and presentations of fundamental groups, and later on to determine these fundamental groups (manual work or Magma). These computations enable us to get some hints about potential Zariski pairs, see examples in [6].

Keywords
Moduli space, Zariski pairs, degenerations, fundamental groups.

References

[1] M. AMRAM, C. GONG, J.-L. MO, "On the Galois covers of degenerations of surfaces of minimal degree". *Mathematische Nachrichten*, **296**(4), 2023, 1351–1365.
https://doi.org/10.1002/mana.202100183.

[2] M. AMRAM, "Non-planar degenerations and related fundamental groups".
https://arxiv.org/abs/2104.02781.

[3] M. AMRAM, C. GONG, P. KUMAR ROY, U. SINICHKIN, U. VISHNE, "The fundamental group of Galois covers of octahedral surfaces".
https://doi.org/10.48550/arXiv.2303.05241

[4] E. R. VAN KAMPEN, "On the fundamental group of an algebraic curve". *Amer. J. Math.*, **55**, (1933), 255–260.

[5] M. AMRAM, R. LAWRENCE, U. VISHNE, "Artin covers of the braid groups". *Journal of Knot Theory and its Ramifications*, **21**(7), (2012).
https://doi.org/10.1142/S0218216512500617

[6] M. AMRAM, R. SHWARTZ, U. SINICHKIN, S.-L. TAN, H.-O. TOKUNAGA, "Zariski pairs of conic-line arrangements of degrees 7 and 8 via fundamental groups".
https://arxiv.org/abs/2106.03507.

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session on *"Algebraic Geometry from an Algorithmic Point of View"*

On the weighted proximity graph of the base locus of a plane Cremona map

Alberto Calabri[1] [clblrt@unife.it]

[1] Department of Mathematics and Computer Science, Università degli Studi di Ferrara, Ferrara, Italy

A plane Cremona map is a birational map $\gamma\colon \mathbb{P}^2 \dashrightarrow \mathbb{P}^2$ of the complex projective plane $\mathbb{P}^2$ in itself. They form the so-called plane Cremona group $\mathrm{Cr}(\mathbb{P}^2)$, also denoted by $\mathrm{Bir}(\mathbb{P}^2)$. In particular, a plane Cremona map γ can be defined by three homogeneous polynomials, with no common factor, of the same degree, that is called the *degree* of γ. The famous Noether-Castelnuovo Theorem states that $\mathrm{Cr}(\mathbb{P}^2)$ is generated by the (linear) automorphisms of $\mathbb{P}^2$ and the elementary quadratic map

$$\sigma\colon \mathbb{P}^2 \dashrightarrow \mathbb{P}^2, \qquad \sigma([x:y:z]) = [yz:xz:xy].$$

Let us say that two plane Cremona maps γ, γ' are *equivalent* if there exist two automorphisms α, β of $\mathbb{P}^2$ such that

$$\gamma' = \alpha \circ \gamma \circ \beta.$$

It was classically very well known that there are exactly three equivalence classes of quadratic planar Cremona map.

A description of equivalence classes of cubic planar Cremona maps has been given in 2013 by D. Cerveau and J. Déserti. They found 32 types of equivalence classes, by studying the plane curves that are contracted by a cubic planar Cremona map. In the paper [1], Nguyen Thi Ngoc Giao and me found a mistake and some inaccuracies in the work by Cerveau and Déserti, and we gave a fine and complete classification of equivalence classes of cubic planar Cremona maps. The main tool of our approach is a new discrete invariant of the base locus of a plane Cremona map, called *weighted proximity graph*. Indeed, in the paper [1], we classify weighted proximity graphs of cubic planar Cremona maps up to isomorphism and, in her Ph.D. Thesis [2], Nguyen Thi Ngoc Giao classified weighted proximity graphs of quartic planar Cremona maps up to isomorphism.

In a work in progress, we are preparing scripts that classify weighted proximity graphs of plane Cremona maps of fixed degree, up to isomorphism, by using several Computer Algebra tools, like Maple, Magma, CoCoA, Macaulay2, Pari-GP, Matlab.

Keywords
Plane Cremona map, base locus, weighted proximity graph

References

[1] A. CALABRI, NGUYEN THI NGOC G., On the classification of cubic planar Cremona maps. *Bull. Soc. Math. France* **150**(4), 625–676 (2022).
[2] NGUYEN THI NGOC G., *On plane Cremona maps of small degree and their quadratic lengths*, Ph.D. thesis, University of Modena and Reggio Emilia, 2020.

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session on *"Algebraic Geometry from an Algorithmic Point of View"*

Irreducible supernatural bundles on Grassmannians

Ozhan Genc[1] [ozhangenc@gmail.com]

[1] Jagiellonian University, Faculty of Mathematics and Computer Science, Kraków, Poland

A vector bundle $\mathcal{E}$ on a polarized variety $(X, \mathcal{O}_X(h))$ of dimension n is called supernatural if for each $j \in \mathbb{Z}$ there is at most one i such that $\mathrm{h}^i(\mathcal{E}(jh)) = 0$ and the Hilbert polynomial of $\mathcal{E}$ has n distinct integral roots. These bundles play a key role in the main results of Boij-Söderberg theory, providing the extremal rays of the cone of cohomology tables[1]. The existence of supernatural bundles for any given root sequence is open for an arbitrary variety even if it is known for $\mathbb{P}^n$. For example, what is the situation for Grassmannians?

A $m \times n$-matrix $M = (a_{ij})$ with coefficients $a_{ij} \in \mathbb{Z}_{>0}$ is a step matrix if the differences between columns and rows are constant.

In this talk, we will explore the answer of the question for irreducible bundles on Grassmannians. We will show that a given set S of $(k+1) \cdot (n-k)$ distinct positive numbers is a root set of an irreducible bundle on the Grassmann variety $G(r, k)$ of k-linear subspaces of $\mathbb{P}^n$ together with the Plücker embedding if and only if one can construct a $(k+1) \times (n-k)$ step matrix using the set S. So, the problem of existence of an irreducible supernatural bundle on Grassmannians is equivalent to the existence of a step matrix.

Additionally, I will mention about a small python package which turns the possible step matrices from a given set if it exists. I will be open the comments from the audience how to improve the efficiency of this code.

Keywords
Supernatural Bundles, Grassmannian, Step matrix

References

[1] D. EISENBUD; F.-O. SCHREYER, Betti numbers of graded modules and cohomology of vector bundles. *J. Amer. Math. Soc.* **22**, 859–888 (2009).

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session on *“Algebraic Geometry from an Algorithmic Point of View”*

An algorithmic approach to characterize Cohen-Macaulay binomial edge ideals of small graphs

***Davide Bolognini*[1], *Antonio Macchia*[2], *Giancarlo Rinaldo*[3],**
Francesco Strazzanti[4] [strazzanti@dima.unige.it]

[1] Dipartimento di Ingegneria Industriale e Scienze Matematiche, Università Politecnica delle Marche, Ancona, Italy
[2] Fachbereich Mathematik und Informatik, Freie Universität Berlin, Berlin, Germany
[3] Dipartimento di Matematica e Informatica, Fisica e Scienze della Terra, Università di Messina, Messina, Italy
[4] Dipartimento di Matematica, Università di Genova, Genoa, Italy

A binomial edge ideal J is an ideal of a polynomial ring generated by some minors of a generic $2 \times n$ matrix. Therefore, it is possible to associate with J a finite simple graph G with n vertices whose edges correspond to the minors generating J.

These ideals were introduced independently in [4] and [6] and have been extensively studied since then. In [4] a combinatorial characterization of the unmixedness of J is given in terms of some special disconnecting sets of vertices of G called *cut sets*. However, giving a description of the algebraic properties of binomial edge ideals in terms of the combinatorics of the associated graphs is usually a challenging problem.

In [3] a characterization of the Cohen-Macaulayness of J has been conjectured using the cut sets of G. The conjecture is known to be true for several classes of graphs, such as bipartite, chordal, and traceable graphs, see [2,3,5,7]. However, the general case is still open.

After an introduction to the topic and to the conjecture above, I will explain how this conjecture can be proved by finding a special vertex in all graphs satisfying a certain property. Looking for this vertex, in [1] we develop an algorithm that allowed us to prove the conjecture for graphs having at most 15 vertices, significantly extending the previous computational results contained in [5]. Several properties proved to develop the algorithm are important also from a theoretical point of view and have allowed to prove the conjecture in other cases.

Keywords
Binomial edge ideal, Cohen-Macaulay, accessible graph, cut set

References

[1] D. BOLOGNINI, A. MACCHIA, G. RINALDO, F. STRAZZANTI, Cohen-Macaulay binomial edge ideals of small graphs, preprint (2022), arXiv:2212.09181.
[2] D. BOLOGNINI, A. MACCHIA, F. STRAZZANTI, Binomial edge ideals of bipartite graphs, *Eur. J. Combin.* **70**, 1–25 (2018).
[3] D. BOLOGNINI, A. MACCHIA, F. STRAZZANTI, Cohen-Macaulay binomial edge ideals and accessible graphs, *J. Algebr. Combin.* **55**, 1139–1170 (2022).
[4] J. HERZOG, T. HIBI, F. HREINSDÓTTIR, T. KAHLE, J. RAUH, Binomial edge ideals and conditional independence statements, *Adv. in Appl. Math.* **45**, 317–333 (2010).
[5] A. LERDA, C. MASCIA, G. RINALDO, F. ROMEO, (S_2)-condition and Cohen-Macaulay binomial edge ideals, *J. Algebr. Comb.* **57**, 589–615 (2023).
[6] M. OHTANI, Graphs and ideals generated by some 2-minors, *Comm. Algebra* **39**, 3, 905–917 (2011).
[7] K. SAHA, I. SENGUPTA, Cohen-Macaulay binomial edge ideals in terms of blocks with whiskers, preprint (2022), arXiv:2203.04652.

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session on *"Algebraic Geometry from an Algorithmic Point of View"*

Sumsets and the Castelnuovo-Mumford regularity of projective monomial curves

Philippe Gimenez[1*], ***Mario González-Sánchez***[1*] [mario.gonzalez.sanchez@uva.es]

[1] Mathematics Research Institute (IMUVA), Univ. of Valladolid, Spain

Given $A = \{a_0, \ldots, a_{n-1}\}$ a finite set of $n \geq 4$ non-negative integers that we will assume to be in normal form, i.e., such that $0 = a_0 < a_1 < \cdots < a_{n-1} = d$ and relatively prime, the s-fold sumset of A is the set sA of integers obtained by collecting all the sums of s elements in A. On the other hand, given an infinite field k, one can associate to A the projective monomial curve $\mathcal{C}_A$ parametrized by A:

$$\mathcal{C}_A = \{(v^d : u^{a_1}v^{d-a_1} : \cdots : u^{a_{n-2}}v^{d-a_{n-2}} : u^d) \in \mathbb{P}_k^{n-1} \mid (u : v) \in \mathbb{P}_k^1\}.$$

In [2], the author proved that the size of the sumsets of A coincide with the values of the Hilbert function of $k[\mathcal{C}_A]$, the coordinate ring of $\mathcal{C}_A$, for all $s \in \mathbb{N}$, i.e., $|sA| = \mathrm{HF}_A(s)$ for all $s \in \mathbb{N}$. This follows the philosophy of [1].

Let $\mathcal{S}_1$ and $\mathcal{S}_2$ denote the numerical semigroups generated by A and $d - A$, respectively, where $d - A = \{d - a : a \in A\}$. Moreover, for $i = 1, 2$ we denote by c_i the conductor of the numerical semigroup $\mathcal{S}_i$, i.e. $c_i = \max(\mathbb{N} \setminus \mathcal{S}_i) + 1$. We consider the set $\mathbf{A} = \{(a, d - a) : a \in A\} = \{(0, d), (a_1, d - a_1), \ldots, (d, 0)\}$ and the subsemigroup $\mathcal{S}$ of $\mathbb{N}^2$ generated by $\mathbf{A}$. It is clear that $\mathcal{S} = \sqcup_{s=0}^{\infty} s\mathbf{A}$ and the sumsets of $\mathbf{A}$ are determined by the ones of A since

$$s\mathbf{A} = \{(\alpha, sd - \alpha) : \alpha \in sA\}, \forall s \in \mathbb{N}, \tag{1}$$

and hence the semigroup $\mathcal{S}$ contains exactly the same information as the sumsets of A. By [5, Thm. 1.1], [2, Prop. 3.4] and equation (1), if we denote $C_i = \mathcal{S}_i \cap [0, c_i - 2]$, $i = 1, 2$, one has that for all $s \gg 0$

$$s\mathbf{A} = \{(i, sd - i),\, i \in C_1\} \sqcup \{(i, sd - i),\, i \in [c_1, sd - c_2]\} \sqcup \{(sd - i, i),\, i \in C_2\}. \tag{2}$$

More precisely, for $s \gg 0$, when we go from $s\mathbf{A}$ to $(s+1)\mathbf{A}$, gaps coming from $\mathcal{S}_1$ move up while gaps coming from $\mathcal{S}_2$ move to the right, and there are no other gaps in $(s+1)\mathbf{A}$ than the ones coming from $s\mathbf{A}$, as shown in Figure 1. We define the *conductor of* $\mathcal{S}$ as the least integer σ such that equation (2) holds for all $s \geq \sigma$.

*This work was supported in part by the grants PID2019-104844GB-I00 and TED2021-130358B-I00 funded by MCIN/AEI/10.13039/501100011033 and by the European Union NextGenerationEU/PRTR. The second author thanks financial support from European Social Fund, *Programa Operativo de Castilla y León*, and *Consejería de Educación de la Junta de Castilla y León*.

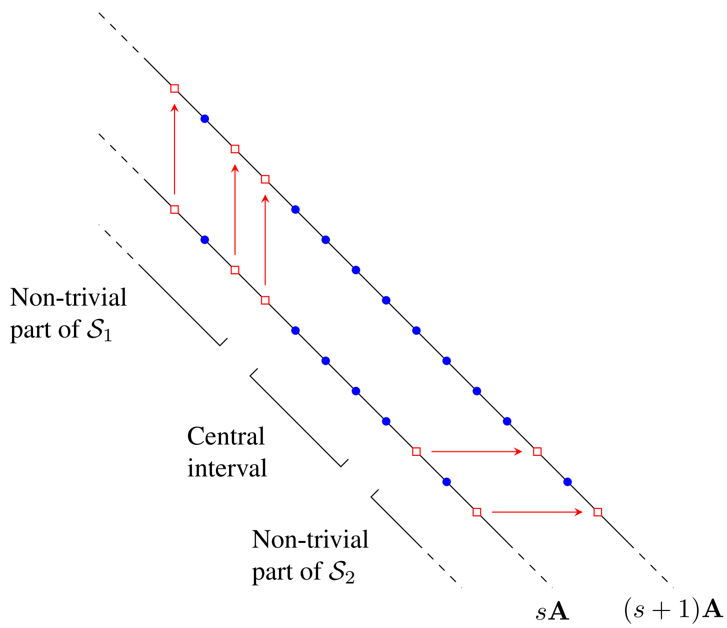


Figure 1: Structure of the sumsets of $\mathbf{A}$. For $s \geq \sigma$, we distinguish three disjoint areas: the central interval and the copies of the non-trivial parts of $\mathcal{S}_1$ and $\mathcal{S}_2$. Here blue points represent points in $\mathcal{S}$ while red squares represent points outside $\mathcal{S}$.

If $k[\mathcal{C}_A]$ is the coordinate ring of $\mathcal{C}_A$ and we denote by $\mathrm{r}\left(k[\mathcal{C}_A]\right)$ the regularity of its Hilbert function, then by [3, Thm. 3.1] the conductor of $\mathcal{S}$ can be computed as

$$\sigma = \max\left\{\mathrm{r}\left(k[\mathcal{C}_A]\right), \left\lceil \frac{c_1 + c_2}{d} \right\rceil\right\}.$$

In order to give a combinatorial formula to calculate the Castelnuovo-Mumford regularity of $k[\mathcal{C}_A]$, we define the two following subsets of the semigroup $\mathcal{S}$, the *Apery set* $\mathrm{AP}_{\mathcal{S}}$ and the *exceptional set* $E_{\mathcal{S}}$:

$$\begin{aligned} \mathrm{AP}_{\mathcal{S}} &= \{(x,y) \in \mathcal{S} : (x-d,y) \notin \mathcal{S}, (x,y-d) \notin \mathcal{S}\}, \\ E_{\mathcal{S}} &= \{(x,y) \in \mathcal{S} : (x-d,y) \in \mathcal{S}, (x,y-d) \in \mathcal{S}, (x-d,y-d) \notin \mathcal{S}\}. \end{aligned}$$

For each $s \in \mathbb{N}$, we consider the 'line' $L_s = \{(x,y) \in \mathbb{N}^2 : x + y = sd\}$ and we denote $\mathrm{AP}_s = \mathrm{AP} \cap L_s$ and $E_s = E_{\mathcal{S}} \cap L_s$. Figure 2 shows how points in $\mathrm{AP}_{\mathcal{S}}$ and $E_{\mathcal{S}}$ look like. Using these notations, we have the following formula which shows the distribution of the elements of $\mathrm{AP}_{\mathcal{S}}$ and $E_{\mathcal{S}}$ in levels [3, Prop. 2.9]:

$$|\mathrm{AP}_s| - |E_s| = |sA| - 2|(s-1)A| + |(s-2)A|, \ \forall s \in \mathbb{N}. \quad (3)$$

By the criterion of Goto et al. [4, Thm. 2.6], $k[\mathcal{C}_A]$ is Cohen-Macaulay if, and only if, $E_{\mathcal{S}} = \emptyset$. Therefore, another equivalent condition of the Cohen-Macaulayness of $k[\mathcal{C}_A]$ is $|\mathrm{AP}_{\mathcal{S}}| = d$ by (3).

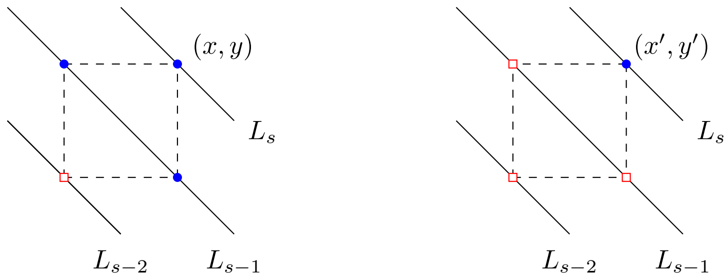


Figure 2: A point (x, y) in E_s and a point (x', y') in AP_s. Here blue points represent points in $\mathcal{S}$ while red squares represent points outside $\mathcal{S}$.

It turns out that $\mathrm{AP}_{\mathcal{S}}$ and $E_{\mathcal{S}}$ are both finite sets and we define the following numbers associated to $\mathcal{S}$ and the monomial curve $\mathcal{C}_A$:

$$m\left(\mathrm{AP}_{\mathcal{S}}\right) = \max\left(\{s : \mathrm{AP}_s \neq \emptyset\}\right) ,$$
$$m\left(E_{\mathcal{S}}\right) = \max\left(\{s : E_{s+1} \neq \emptyset\}\right) \text{ (and } m\left(E_{\mathcal{S}}\right) = -\infty \text{ if } E_{\mathcal{S}} = \emptyset) .$$

These definitions allow us to give a combinatorial formula for the Castelnuovo-Mumford regularity of $k[\mathcal{C}_A]$ [3, Thm. 3.6]:

$$\operatorname{reg}\left(k[\mathcal{C}_A]\right) = \max\{m\left(\mathrm{AP}_{\mathcal{S}}\right), m\left(E_{\mathcal{S}}\right)\} .$$

Finally, we can bound the Castelnuovo-Mumford regularity of $k[\mathcal{C}_A]$ from above and from below in terms of the conductor of $\mathcal{S}$ [3, Thm. 3.15]:

1. If $\sigma = \mathrm{r}\left(k[\mathcal{C}_A]\right) \geq \lceil \frac{c_1+c_2}{d} \rceil$, then $\sigma \leq \operatorname{reg}\left(k[\mathcal{C}_A]\right) \leq \sigma + 1$.
2. If $\sigma = \lceil \frac{c_1+c_2}{d} \rceil > \mathrm{r}\left(k[\mathcal{C}_A]\right)$, then $\lceil \frac{\sigma}{2} \rceil + 1 \leq \operatorname{reg}\left(k[\mathcal{C}_A]\right) \leq \sigma + 1$.

Keywords
projective monomial curve, semigroup ring, Castelnuovo-Mumford regularity, sumsets, Apery set

References

[1] S. ELIAHOU; E. MAZUMDAR, Iterated sumsets and Hilbert functions. *J. Algebra* **593**(1), 274–294 (2022).
[2] J. ELIAS, Sumsets and Projective Curves. *Mediterr. J. Math.* **19**(177), 1–11 (2022).
[3] P. GIMENEZ; M. GONZÁLEZ-SÁNCHEZ, Castelnuovo-Mumford regularity of projective monomial curves via sumsets. *arXiv:2304.10989v1*, 1–18 (2023).
[4] S. GOTO; N. SUZUKI; K. WATANABE, On affine semigroup rings. *Japan. J. Math.* **2**(1), 1–12 (1976).
[5] M. B. NATHANSON, *Additive Numer Theory: Inverse Problems and the Geometry of Sumsets*. Springer-Verlag, New York, 1996.

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session on *“Algebraic Geometry from an Algorithmic Point of View”*

Applying machine learning to the computation of Pommaret bases — A progress report

Amir Hashemi[1]***, Mahshid Mirhashemi***[1]***,***
Werner M. Seiler[2] [seiler@mathematik.uni-kassel.de]

[1] Department of Mathematical Sciences, Isfahan University of Technology, Isfahan 84156-83111, Iran
[2] Institute of Mathematics, Kassel University, 34109 Kassel, Germany

Involutive bases are Gröbner bases with additional combinatorial properties and arose from merging ideas from computer algebra with the Janet–Riquier theory of differential equations [1]. Any involutive basis induces a combinatorial decomposition of the ideal giving immediately the Hilbert function of the ideal. The involutive theory also leads to an alternative algorithm for the construction of involutive / Gröbner bases which is competitive to advanced variants of the Buchberger algorithm. For a comprehensive review of algorithmic and theoretical aspects of involutive bases, we refer to [2,3].

Pommaret bases (for the `degrevlex` term order) are a special instance of involutive bases which are of particular interest for algebraic geometry. Compared to arbitrary Gröbner bases, they reflect much better algebraic and geometric properties of the ideal they generate. Many invariants – some of which are expensive to compute with standard methods – can be directly read off from a Pommaret basis, for example the Krull dimension (together with a maximal set of independent variables), the depth/projective dimension (together with a maximal regular sequence), the Castelnuovo–Mumford regularity (and more generally all extremal Betti numbers), the satiety (plus the saturation) or a parameter ideal. A Pommaret basis also provides simple tests whether an ideal is Cohen–Macaulay, Gorenstein or componentwise linear. On a more theoretical side, Pommaret bases allow for constructive proofs of for example Hilbert's syzygy theorem, the existence of Noether normalisations, Hironaka's criterion for Cohen–Macaulay rings or the criteria for q-regularity by Bayer–Stillman and Eisenbud–Goto, respectively. For more details, we refer to [2,4].

Many of these results are a consequence of the fact that a Pommaret basis induces a free resolution of the ideal it generates. The shape of the resolution can be immediately deduced from the Pommaret basis. Using tools from discrete Morse theory, one can also efficiently determine the differentials [5].

From a computational point, Pommaret bases face a problem: they exist only in suitable coordinates. More precisely, an ideal has a finite Pommaret basis, if and only if its leading ideal is quasi-stable (in this case, we say that the ideal is in *quasi-stable position*) [2,4]. In fact, many of the above mentioned results are due to this property, as they require a generic position. One can show that a *random* linear transformation produces with probability 1 quasi-stable position. However, random transformations destroy all sparsity in the basis and thus are not useful computationally.

A first *deterministic* approach to this problem was proposed in [6] (in the context of differential equations); however, the proof contained gaps. An improved version was presented in [2,4] and a complete and detailed proof finally given in [7]. The basic idea is to employ repeatedly very sparse transformations, so-called *elementary moves*, until a quasi-stable position is reached. There exist different methods to find suitable elementary moves. One can for example compare the Janet and the Pommaret multiplicative variables of each generator (in a Janet basis) or one can determine obstructions to quasi-stability from a minimal basis of the leading ideal. Typically, several elementary moves are suitable and while each choice will lead after finitely many steps to a quasi-stable position, the efficiency of the process will depend on the made choice.

Such situations are quite common in computer algebra: the correctness and the termination of an algorithm is independent of certain choices made during its execution, but its efficiency strongly depends on these choices. A classical example is the choice of the next S-polynomial in Buchberger's algorithm. Classically, one then relies on some – typically fairly simple – heuristics to make the required choices. Machine learning provides here an alternative approach without affecting the mathematical correctness of the results. In the case of Buchberger's algorithm, the authors of [8] used a 1D convolutional neural network, i. e. a variant of reinforcement learning, to choose S-polynomials in Gröbner bases computations for binomial ideals.

A group of authors studied in a series of articles including [9,10] the problem of choosing a good variable ordering for cylindrical algebraic decomposition. Here, one faces the same problem: the correctness of the results in independent of the used ordering, but the runtime of the computations will dependent very strongly on it. The authors formulated the choice of an ordering as a multi classification problem for which many algorithmic approaches like support vector machines have been developed in machine learning.

We will report on first results in applying similar ideas to the deterministic construction of "good" coordinates for Pommaret bases within the deterministic algorithm presented in [7]. This algorithm starts with a Gröbner basis in the current coordinate system. If the leading ideal is not quasi-stable, then an elementary move related to an obstruction is performed and a Gröbner basis of the transformed ideal is computed. This process is iterated until a quasi-stable position is reached. Termination of this algorithm was shown in [7] independent of how the used elementary moves are chosen. Experiments with various heuristics in prototype implementations were inconclusive.

We now propose to use machine learning for choosing the next elementary move to be performed. The goal is to predict which move yields the greatest increase of the volume polynomial of the Pommaret span of the current basis. Analogously to [9,10], we consider this as a multi classification problem (with a class corresponding to a choice of an elementary move) and compare five approaches to its solution: support vector machines, k-nearest neighbours, decision trees, multilayer perceptrons and logistic regression.

A great problem in applying methods from machine learning in the context of commutative algebra and algebraic geometry is the generation of training data, as there do not exist sufficiently large databases of "typical" ideals that could be used for training purposes. Hence, the only possibility is to generate random ideals, although it is well-known that these are not necessarily representative for the type of ideals appearing in applications. We wrote our own ideal generator where the number of generators in the basis, the number of terms in each generator and the degree of each generator follow a Poisson distribution. With this generator, we produced 10.000 ideals in a polynomial ring with four variables.

For the machine learning, each ideal is represented by a feature vector. The largest part of this vector consists of "statistical" information encoding degrees (total and in individual variables) or the appearence of the different variables in the generators and their leading terms. A smaller "transformation" part lists which elementary moves are proposed by the obstructions to quasi-stability of the leading ideal. In four variables, this leads to about 100 integer entries in the feature vector.

In 4 variables, 6 different elementary moves exist. For preparing the training data, each ideal was transformed with each elementary move, then a Janet basis was computed of the transformed ideal and finally the volume polynomial of the Pommaret span of this basis was determined. A comparison of the results showed which elementary move is optimal. Hyperparameters of the different methods were as usually determined via cross-validation.

First experiments showed promising results. The accuracy of the different methods varied between 75% and 90% with support vector machines giving clearly the best and k nearest neighbours the worst results. In a comparison with random choices, a support vector machine was better in about 55% of the examples and produced the same results in more than 30% of the examples. We expect that the ratio will be even more in favour of machine learning, if the number of variables and hence the number of possible elementary moves increases.

The experiments also lead to some theoretical "surprises". We expected that only elementary moves related to obstructions of quasi-stability are useful and originally intended to take into account only these. However, in our sample of random ideals we found several cases where an unrelated move was not only useful but in fact even the optimal choice. We still need a deeper understanding of this observation.

Future works will include studies of ideals in a larger number of variables. An important goal will be to include also transpositions as allowed transformation and to take the sparsity of the obtained basis into account. We also want to use a more quantitative way to analyse the results. This means not just to mark whether the optimal choice was found, but to measure how much worse the actual choice was.

Keywords
Pommaret bases, quasi-stable position, deterministic coordinate transformations, machine learning, multi classification

References

[1] V.P. GERDT; Y.A. BLINKOV, Involutive bases of polynomial ideals. *Math. Comput. Simul.* **45**(5–6), 519–541 (1998).
[2] W.M. SEILER, *Involution – The Formal Theory of Differential Equations and its Appli-*

cations in Computer Algebra. Algorithms and Computation in Mathematics 24, Springer-Verlag, Berlin, 2010.
[3] W.M. SEILER, A Combinatorial Approach to Involution and δ-Regularity I: Involutive Bases in Polynomial Algebras of Solvable Type. *Appl. Alg. Eng. Comm. Comp.* **20**(3-4), 207–259 (2009).
[4] W.M. SEILER, A Combinatorial Approach to Involution and δ-Regularity II: Structure analysis of polynomial modules with Pommaret bases. *Appl. Alg. Eng. Comm. Comp.* **20**(3-4), 261–338 (2009).
[5] M. ALBERT, M. FETZER, E. SÁENZ-DE-CABEZÓN, W.M. SEILER, On the Free Resolution Induced by a Pommaret Basis. *J. Symb. Comp.* **68**(2), 4–26 (2015).
[6] M. HAUSDORF, W.M. SEILER, An Efficient Algebraic Algorithm for the Geometric Completion to Involution. *Appl. Alg. Eng. Comm. Comp.* **13**(3), 163–207 (2002).
[7] A. HASHEMI, M. SCHWEINFURTER, W.M. SEILER, Deterministic Genericity for Polynomial Ideals. *J. Symb. Comp.* **86**(2), 20–50 (2018).
[8] D. PEIFER, M. STILLMAN, D. HALPERN-LEISTNER, Learning Selection Strategies in Buchberger's algorithm. *Proc. Machine Learning Research* **119**, 7575–7585 (2020).
[9] M. ENGLAND, D. FLORESCU, Comparing Machine Learning Models to Choose the Variable Ordering for Cylindrical Algebraic Decomposition. In *Intelligent Computer Mathematics – CICM 2019*, C. Kaliszyk, E. Brady, A. Kohlhase, C.S. Coen (eds.). Lecture Notes in Computer Science 11617, Springer-Verlag, Cham, 2019.
[10] Z. HUANG, M. ENGLAND, D.J. WILSON, J. BRIDGE, J.H. DAVENPORT, L.C. PAULSON, Using Machine Learning to Improve Cylindrical Algebraic Decomposition. *Math. Comp. Sci.* **13**, 461–488 (2019).

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session on *"Effective ideal theory and combinatorial techniques in commutative and non commutative rings and their applications"*

A breakthrough concerning the solution of a famous equation on finite fields and its impacts in the context of S-boxes in symmetric cryptography

Sihem Mesnager[1] [smesnager@univ-paris8.fr]

[1] Department of Mathematics, Universities of Paris VIII and Sorbonne Paris Cité, LAGA, CNRS, France.

In this talk, we present some results from a recent (2020-2022) selection: achievements and collections of published articles obtained in [5,9,11]. Finding the number of solutions to equations over finite fields becomes a crucial and unavoidable task that we often encounter when we solve problems algebraically in the domain of protection information theory, basically represented by cryptography and coding theory. More importantly, solving equations over finite fields is a much more important problem from both theoretical and practical points of view. Until recently, we could get satisfied with the number of solutions and not with the complete resolutions of the equations (that is to say, by explicitly finding the set of solutions). This contentment with these shreds of information on the equations that come to us from the problems of the algebraic theory of linear codes or the theory of cryptographic functions in symmetric cryptography becomes more and more unsatisfactory. It becomes important +2022 to seek to develop tools and implement methods to resolve as many equations over finite fields as possible and make them available to theorists, cryptographers and coding theory.

We discuss solving algebraic equations over finite fields. Precisely we shall focus on one equation and, namely, be interested in the problem of solving the equation $P_a(X) = 0$ explicitly over the finite field $\mathbb{F}_Q$, where $P_a(X) := X^{q+1} + X + a$, $Q = p^n$, $q = p^k$, $a \in \mathbb{F}_Q^*$ and p is a prime. This problem arises in many contexts, including correcting codes and cryptographic functions. The resolution of $P_a(X) = 0$ was a long research open problem for over half of a century. The research on this specific problem has a long history of more than a half-century from the year 1967 when Berlekamp, Rumsey and Solomon first considered a very particular case with $k = 1$ and $p = 2$. After that, many efforts were made by several researchers (such as Helleseth and Kholosha in 2008 and 2010 ([6, 7]), Bracken, Tan and Tan in 2014 ([3,4])) toward identifying all the $\mathbb{F}_Q$-zeros of $P_a(X)$ specifically for a particular problem instance over binary fields, i.e. $p = 2$. Let N_a denote the number of zeros in $\mathbb{F}_Q$ of the polynomial $P_a(X)$ and M_i denote the number of $a \in \mathbb{F}_Q^*$ such that $P_a(X)$ has exactly i zeros in $\mathbb{F}_Q$. In 2004, Bluher [1] proved that N_a equals 0, 1, 2 or $p^d + 1$ where $d = \gcd(k, n)$

and computed M_i for every i. She also stated some criteria for the number of the $\mathbb{F}_Q$-zeros of $P_a(X)$.

The number of roots of any projective polynomial was determined implicitly in [8] and explicitly in [14] from its coefficients. In particular, new criteria for which $P_a(X)$ has 0, 1, 2 or p^d+1 roots were proved in [14] for any characteristic. After that, many efforts were made by several researchers (namely, Helleseth and Kholosha in 2008 and 2010 and next, Bracken, Tan and Tan in 2014) toward identifying all the $\mathbb{F}_Q$-zeros of $P_a(X)$ specifically for a particular problem instance over binary fields, i.e. $p=2$.

In this talk, we shall restrict ourselves to the even characteristic. In the first part of this talk, we will see that the resolution of $P_a(X) := X^{2^k+1}+X+a=0$ was like a puzzle where almost all the ingredients have been introduced in the literature, and almost all had to be put together using new ideas and appropriate algebraic techniques. Specifically, we first show how we have very recently, [10] completely solved the equation $P_a(X) := X^{2^k+1}+X+a=0$ over $\mathbb{F}_{2^n}$ when $d=1$. We will show, in particular, using a new Identity of Dickson polynomials given by Bluher [2], that the problem of finding zeros in $\mathbb{F}_{2^n}$ of $P_a(X)$ can be divided into two problems with odd k: to find the unique preimage of an element in $\mathbb{F}_{2^n}$ under a M$\ddot{u}$ller-Cohen-Matthews polynomial and to find preimages of an element in $\mathbb{F}_{2^n}$ under a Dickson polynomial. By completely solving these two independent problems, they explicitly calculated all possible zeros in $\mathbb{F}_{2^n}$ of $P_a(X)$, with new criteria for which N_a is equal to 0, 1 or 3 as a by-product. We highlight some of the latest important achievements listed above that could not be found without the precious advances made by Bluher [1,2]. Also, the resolution of the equation $P_a(X)=0$ was made later in two papers in any characteristic p without any restriction on p and $\gcd(n,k)$. Thus now the equation $X^{p^k+1}+X+a=0$ over $\mathbb{F}_{p^n}$ is completely solved for any prime p, any integers n and k.

In the second part of this talk, we shall present two applications where our was crucial. The first one is to provide in [5] a direct proof of the APN-ness of the Kasami functions. And the second one was to provide ([11]) a complete characterisation of quadrinomials permutations on the finite field $\mathbb{F}_{4^m}$ of shape $f_{\underline{\epsilon}}(X) := \epsilon_1\overline{X}^{q+1}+\epsilon_2\overline{X}^{q}X+\epsilon_3\overline{X}X^q+\epsilon_4X^{q+1}$, definitively (where $q=2^k$, $Q=2^m$, m is odd, $\gcd(m,k)=1$, $\overline{X}=X^Q$). As a direct application, we derive a complete proof of the conjecture proposed in [13] and confirm its validity by presenting a complete proof of the bijectivity of $f_{\underline{\epsilon}}$ over $\mathbb{F}_Q$ without any restriction. Solving this conjecture gives rise to a family of promising candidates with excellent cryptographic properties as S-boxes in designing block ciphers in symmetric cryptography, namely, permutations having boomerang uniformity 4 and the best-known nonlinearity. The considered conjecture proved in [11] has attracted much attention in recent years (2019-2021). As seen in the very recent literature, more than 7 papers published in IEEE-IT and DCC journals appeared proposing exciting approaches to solve this conjecture. Still, unfortunately, despite these efforts, the conjecture remains unsolved on its whole. However, it is the first time we have offered an approach that solves the enter conjecture by simultaneously handling both sides involving equivalence. Very recently [12], we presented a complete proof of the bijectivity of $f_{\underline{\epsilon}}$ over $\mathbb{F}_{Q^2}$ without any restriction. This is joint work with Kwang Ho Kim and some of his team members cited in the references.

Keywords
Equation, M$\ddot{u}$ller-Cohen-Matthews (MCM) polynomials, Dickson polynomial, Zeros of poly-

nomials

References

[1] A.W. Bluher On $x^{q+1}+ax+b$, *Finite Fields and Their Applications*, **10**(3), 285 – 305 (2004).
[2] A.W. Bluher A New Identity of Dickson Polynomials. *ArXiv:1610.05853 [math.NT]* (2016).
[3] C. Bracken and T. Hellesetha Triple-error-correcting BCH-like codes. in: *IEEE Int. Symp. Inf. Theory*, 1723 – 1725 (2009).
[4] C. Bracken, C.H. Tan and Y. Tan On a class of quadratic polynomials with no zeros and its application to APN functions, *Finite Fields and Their Applications*, **25**, 26 – 36 (2014).
[5] C. Carlet, K.H. Kim, and S. Mesnager A direct proof of APN-ness of the Kasami functions. *Des. Codes Cryptogr.*, **89**(3), 441–446 (2021).
[6] T. Helleseth, and A. Kholosha, On the equation $x^{2^l+1}+x+a$ over $GF(2^k)$. *Finite Fields and Their Applications*, **14**(1), 159–176 (2008).
[7] T. Helleseth, and A. Kholosha $x^{2^l+1}+x+a$ and related affine polynomials over $GF(2^k)$. *Cryptogr. Commun.*, **2**, 85 – 109 (2010).
[8] J. von zur Gathen, M. Giesbrecht, K. Ziegler Composition collisions and projective polynomials, in: *ISSAC*, 2010, 123–130.
[9] K.H. Kim, J. Choe and S. Mesnager Solving $X^{q+1}+X+a=0$ over finite fields. *Finite Fields and Their Applications*, **70** 101797, 2021.
[10] K.H. Kim and S. Mesnager Solving $x^{2^k+1}+x+a=0$ in $\mathbb{F}_{2^n}$ with $\gcd(n,k)=1$. *Finite Fields and Their Applications*, **63** 101630 (2020).
[11] K.H. Kim, S. Mesnager, J.H. Choe, D.N. Lee, S. Lee, and M.C. Jo On permutation quadrinomials with boomerang uniformity 4 and the best-known nonlinearity. *Des. Codes Cryptogr.* **90**(6), 1437-1461 (2022).
[12] K.H. Kim, S. Mesnager, C. H. Kim, and M.C. Jo. Completely Characterizing a Class of Permutation Quadrinomials. Submitted to *Finite Fields and Their Applications*, April 2022.
[13] K. Li, C. Li, T. Helleseth, and L. Qu. Cryptographically strong permutations from the butterfly structure. *Designs, Codes and Cryptography*, **89**, 737–761, (2021).
[14] G. McGuire and J. Sheekey. A characterization of the number of roots of linearized and projective polynomials in the field of coefficients. *Finite Fields and Their Applications*, **57**, 68– 91 (2019).

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session on *“Effective ideal theory and combinatorial techniques in commutative and non commutative rings and their applications”*

A new view on the Rees algebra of a monomial plane curve parametrization

***Rodrigo Iglesias*[1], *Matthias Orth*[2], *Eduardo Sáenz-de-Cabezón*[1], *Werner M. Seiler*[2]**
[morth@mathematik.uni-kassel.de]

[1] Grupo de Informática, Universidad de La Rioja, Logroño, Spain
[2] Institute of Mathematics, Kassel University, Kassel, Germany

A monomial curve in the projective plane $\mathbb{P}^2_{\mathbb{K}}$ is an algebraic curve parameterized by a map $p : \mathbb{P}^1_{\mathbb{K}} \longrightarrow \mathbb{P}^2_{\mathbb{K}}, (T_0 : T_1) \mapsto (T_0^d : T_0^u T_1^{u-d} : T_1^d)$, where $d \in \mathbb{Z}_{>1}$ is the degree of the curve and u is coprime to d. To the parameterization p, we associate the monomial ideal $I = \langle T_0^d, T_0^u T_1^{u-d}, T_1^d \rangle$. The Rees algebra associated to I is $\mathcal{R}_I = \oplus_{m \geq 0} I^m \cdot z^m \subset \mathbb{K}[T_0, T_1, z]$, where z is a new variable. The Rees ideal is the kernel of the ring homomorphism ϕ : $\mathbb{K}[T_0, T_1, X_0, X_1, X_2] \to \mathbb{K}[T_0, T_1, z]$, defined by:

$$\begin{aligned} X_0 &\mapsto T_0^d z, \\ X_1 &\mapsto T_0^u T_1^{d-u} z, \\ X_2 &\mapsto T_1^d z. \end{aligned}$$

Similarly, one can define monomial curves in projective spaces of higher dimensions. The structure of the Rees algebra and its minimal free resolution is best known for plane curves. Indeed, [3] shows how to compute the minimal bigraded resolution of the Rees Algebra associated to a monomial plane curve. In that work, slow Euclidean remainder sequences derived from the degrees d and u appearing in the generators of I are used to decribe the module homomorphisms in the free resolution. Moreover, by [5] it is known that there exists an approach to derive the resolution via geometric means, because the ideal I can be viewed as a codimension 2 lattice ideal.

In our work, we derive the minimal generators of the Rees ideal and the minimal free resolution via a new approach that combines algorithmic and geometric ideas. In order to obtain the minimal generators, we exploit the structure of the cyclic subgroup generated by $[u] \in \mathbb{Z}/d\mathbb{Z}$. From the minimal binomial generating set, using a degree reverse lexicographic term ordering $<$ with $T_0 < T_1 < X_0 < X_2 < X_1$, we obtain a Gröbner basis of the Rees ideal by adding only the trivial relation $T_0^d X_2 - T_1^d X_0$. To this Gröbner basis, we associate a directed graph with the Gröbner basis elements as nodes and suitable edge labels derived from the generators connected by the edges. We show that a complete free resolution can be read off from this graph and that the minimal free resolution is obtained just by deleting certain nodes from the graph.

We conclude with some remarks on whether we can expect our methods to apply also to Rees ideals of monomial curves in $\mathbb{P}_{\mathbb{K}}^m$ with $m \geq 3$. Such monomial curves have been studied for a long time (see e.g. [1], [2]); however, the analysis of the structure of their Rees algebras remains a difficult problem. We expect that our approach will be useful for determining coarser invariants like for example the projective dimension without much computational effort. However, the description of the whole resolution for such curves remains as a topic for future work.

Keywords
Monomial curves, Rees algebras, syzygy modules, free resolutions

References

[1] M. BARILE; M. MORALES, On the equations defining projective monomial curves. *Commun. Algebra* **26**(6), 1907–1912 (1998).
[2] H. BRESINSKY, Minimal free resolutions of monomial curves in $\mathbb{P}_k^3$. *Linear Algebra Appl.* **59**, 121–129 (1984).
[3] T. CORTADELLAS BENÍTEZ; C. D'ANDREA, The Rees algebra of a monomial plane parametrization. *J. Symb.. Comput.* **70**, 71–105 (2015).
[4] M. DIPASQUALE; C.A. FRANCSCICO; J. MERMIN; J. SCHWEIG; G. SOSA, The Rees algebra of a two-Borel ideal is Koszul. *Proc. Am. Math. Soc.* **147**(2), 467–479 (2019).
[5] I. PEEVA; B. STURMFELS, Syzygies of codimension 2 lattice ideals. *Math. Z.* **229**(1), 163–194 (1998).

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session on *"Effective ideal theory and combinatorial techniques in commutative and non commutative rings and their applications"*

Marked bases for some quotient rings and applications - part I

Cristina Bertone[1]***, Francesca Cioffi***[2]***, Matthias Orth***[3]***,***
Werner M. Seiler[3] [cristina.bertone@unito.it]

[1]Dipartimento di Matematica, University of Turin, 10123 Turin, Italy
[2]Dipartimento di Matematica e Appl., University of Naples Federico II, 80126 Naples, Italy
[3]Institute of Mathematics, University of Kassel, 34109 Kassel, Germany.

Marked bases on a quasi-stable ideal are polynomial bases for ideals in the polynomial ring $R = \mathbb{K}[x_0, \ldots, x_n]$, $\mathbb{K}$ a field, that share some good properties of Groebner bases. Marked bases are term order free, but the role of the initial ideal is played by the quasi-stable ideal we consider, and its combinatorial properties somehow replace the term order.

Marked bases over a quasi-stable ideal were used to study Hilbert and Quot schemes (see for instance [1]), which are "mysterious"objects in algebraic geometry. Due to this application, it is quite natural to consider ideals in R/I, for I homogeneous ideal, and look for reasonable polynomial bases for them in order to deal with the Hilbert scheme on $\mathrm{Proj}(R/I)$.

We can do this in two different ways. The first one works in quotient rings R/I, where I is a homogeneous ideal, and exploits the good behaviour of quasi-stable ideals with respect to saturations. However, it requires the computation of the equations defining a complete marked scheme, and then adding some more constraints.

The second one is inspired by a recent paper [3]. We generalize the notion of marked basis over a quasi-stable ideal to quotient rings R/I, with I a quasi-stable ideal, by defining *relative* marked basis w.r.t. I. We obtain algorithms to verify that a given marked set is a relative marked basis w.r.t. I and to compute the affine scheme parameterizing relative marked bases w.r.t. I. These algorithms are more effective than the techinique developed in the first case, because we need to use a smaller number of parameters in the computations.

This second approach allowed some applications to the Hilbert scheme on $\mathrm{Proj}(R/I)$, with some further hypotheses on I: if I is Cohen-Macaulay, it allows to obtain an open cover of the Hilbert scheme; if I is Macaulay-Lex, it allows to study the smoothness of the lexicographical point. Both applications are discussed in a talk by Francesca Cioffi (part II).

This talk is based on a recent work available at [2].

Keywords
monomial quotient rings, quasi-stable ideal, marked bases.

References

[1] M. Albert, C. Bertone, M. Roggero, W.M. Seiler, Computing Quot schemes via marked bases over quasi-stable modules, *Journal of Algebra*, **550**, 432-470 (2020). [2] C. Bertone, F. Cioffi, M. Orth, W.M. Seiler, Hilbert schemes over quotient rings via relative marked bases, arXiv:2203.11770 [math.AC].
[3] A. Hashemi, M. Orth, W.M. Seiler, Relative Gröbner and Involutive Bases For Ideals In Quotient Rings, *Math. Comput. Sci.* **15**, no. 3, 453-482 (2021)

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session on *"Effective ideal theory and combinatorial techniques in commutative and non commutative rings and their applications"*

Marked bases for some quotient rings and applications - part II

***Cristina Bertone*[1], *Francesca Cioffi*[2], *Matthias Orth*[3], *Werner Seiler*[3]** [cioffifr@unina.it]

[1]Dipartimento di Matematica, University of Turin, 10123 Turin, Italy
[2]Dipartimento di Matematica e Appl., University of Naples Federico II, 80126 Naples, Italy
[3]Institute of Mathematics, University of Kassel, 34109 Kassel, Germany.

Let $R = \mathbb{K}[x_0, \ldots, x_n]$ be the polynomial ring over a field $\mathbb{K}$ in $n+1$ variables and X be the projective closed scheme defined in $\mathbb{P}^n_{\mathbb{K}}$ by the quotient ring R/I over a homogeneous ideal I of R. Exploiting the theory of marked bases, some new computational tools have recently been developed to analyse the Hilbert scheme over X, when I is a quasi-stable ideal. The description of this development will be given in a talk by Cristina Bertone (part I). The present talk will focus on two applications of these tools, under some further hypotheses on the ideal I.

Both the applications take benefits from the fact that the use of marked bases allows the construction of some open subschemes in the Hilbert scheme over X.

When the field $\mathbb{K}$ is infinite and the quotient ring on the quasi-stable ideal I is Cohen-Macaulay, we develop this feature to describe an open cover of Hilbert schemes over such a quotient ring. This first application is achieved thanks to suitable changes of variables applied on open subsets parametrising relative marked bases. We generalize the method which is described in [1] and which is based on deterministically computable suitable linear changes of variables (see [4]). The novelty of this approach consists in the fact that we show that there are computable linear changes of variables of the quotient ring which by definition preserve the complete structure of the ideal I, instead of destroying it.

The second application gives examples of both smooth and singular lex-points in Macaulay-Lex quotient rings, even when $\mathbb{K}$ is not infinite or the quotient ring is not Cohen-Macaulay. Indeed, every non-empty Hilbert scheme over a Macaulay-Lex ring on a quasi-stable ideal has the lex-point. Differently from the case of a Hilbert scheme over a polynomial ring on a field (see [6]), in this case the lex-point can be singular. Also in this case the availability of the open subschemes described by means of the relative marked bases has a crucial role. The benefits obtained by the use of relative marked bases are appreciable even when we count the number of parameters involved in the computations, as we highlight throughout the descriptions of some of our examples. Computational evidences encourage to think that the lex-point is in particular singular in Clements-Lindström rings (see [3] for this kind of ring). The problem of the smoothness of the lex-point is also studied in other Hilbert schemes, see for instance [5].

This talk is based on a recent work available at [2].

Keywords
Marked basis, Hilbert scheme, Cohen-Macaulay ring, Macaulay-Lex ring, open cover, lex-point

References
[1] MARIO ALBERT, CRISTINA BERTONE, MARGHERITA ROGGERO, AND WERNER M. SEILER, Computing Quot schemes via marked bases over quasi-stable modules, *J. Algebra* **550** (2020), 432–470.
[2] CRISTINA BERTONE, FRANCESCA CIOFFI, MATTHIAS ORTH AND WERNER M. SEILER, Open Covers and Lex Points of Hilbert schemes over quotient rings via relative marked bases, available at arXiv:2203.11770.
[3] G. F. CLEMENTS, B. LINDSTRÖM, A generalization of a combinatorial theorem of Macaulay. *J. Comb. Theory* **7**, 230–238 (1969).
[4] AMIR HASHEMI, MICHAEL SCHWEINFURTER, WERNER SEILER, Deterministic genericity for polynomial ideals, *Journal of Symbolic Computation* **86** (2018) 20–50.
[5] RITVIK RAMKUMAR AND ALESSIO SAMMARTANO, On the smoothness of lexicographic points on Hilbert schemes, *J. Pure Appl. Algebra* **226** (2022), no. 3, Paper No. 106872, 12.
[6] ALYSON REEVES AND MIKE STILLMAN, Smoothness of the lexicographic point, *J. Algebraic Geom.* **6** (1997), no. 2, 235–246.

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session on *"Effective ideal theory and combinatorial techniques in commutative and non commutative rings and their applications"*

Vanishing ideals and evaluation codes

Philippe Gimenez[1]***, Diego Ruano***[1]***, Rodrigo San-José***[1] [rodrigo.san-jose@uva.es]

[1] IMUVA-Mathematics Research Institute, Universidad de Valladolid, 47011 Valladolid, Spain

Let $\mathbb{F}_q$ be a finite field of q elements. A code C over $\mathbb{F}_q$ of length n is a vector space $C \subset \mathbb{F}_q^n$. Evaluation codes are codes obtained by evaluating a certain set of polynomials in a given set of points, usually in the affine space $\mathbb{A}^m$. These codes have been used successfully for many applications [1,2] because of their rich algebraic structure, which allows to study their parameters, self-orthogonality properties, etc. Obtaining long codes with good parameters over a fixed finite field in general is a difficult problem. One idea to obtain longer codes over the same finite field while maintaining the algebraic structure of evaluation codes is to evaluate in points of the projective space $\mathbb{P}^m$ [6,9]. In particular, the family of projective Reed-Muller type codes $C_{\mathbb{X}}(d)$, which is obtained by evaluating the set of homogeneous polynomials of degree d in a set $\mathbb{X} \subset \mathbb{P}^m$, provides a nice connection between coding theory and commutative algebra [7,8]. In fact, it is possible to derive the basic parameters of the code $C_{\mathbb{X}}(d)$ from invariants of the vanishing ideal of $\mathbb{X}$, denoted by $I(\mathbb{X})$. Moreover, it is also possible to describe the generalized Hamming weights of the code using the generalized minimum distance function of the vanishing ideal, and using the generalized footprint function, which is easier to compute, one can also obtain a lower bound for the generalized Hamming weights [5].

Therefore, we see that the vanishing ideal $I(\mathbb{X})$ plays a crucial role in studying this family of codes. The set of points $\mathbb{X}$ is usually given as the projective variety defined by a homogeneous ideal I, and one may wonder how to compute $I(\mathbb{X})$ from I. This computation is usually done by adding the equations of the projective space $I(\mathbb{P}^m)$ to I and computing the radical. We give an alternative and more efficient way of computing the vanishing ideal $I(\mathbb{X})$ by using the saturation with respect to the homogeneous maximal ideal [3].

Another approach to study these codes, which can be more fruitful for some applications, is to fix the representatives of the points of $\mathbb{X}$. For instance, we can choose the set formed by the representatives of the points of $\mathbb{X}$ which have the first nonzero coordinate equal to 1, which we denote by X. We can regard X as a subset of $\mathbb{A}^{m+1}$, and we can simply consider the evaluation of the polynomials in S_d at the set X. This approach connects the code $C_{\mathbb{X}}(d)$ with the vanishing ideal $I(X)$ with similar relations to the ones we had between $C_{\mathbb{X}}(d)$ and $I(\mathbb{X})$ before. In this case, given a homogeneous ideal I and the variety that it defines over the projective space $\mathbb{X}$, it is not difficult to obtain the ideal $I(X)$. In fact, we are able to obtain a universal Gröbner basis for $I(X)$ for some sets X, and we give a way to reduce any monomial with respect to this basis. These tools can be used in order to provide bases for the subfield subcodes of projective Reed-Solomon codes and projective Reed-Muller codes, which in turn can be used to obtain classical and quantum codes with good parameters [4].

Keywords
Vanishing ideal, saturation, coding theory, evaluation codes

Acknowledgements
This work was supported in part by the following grants: PID2019-104844GB-I00 funded by MCIN/AEI/10.13039/501100011033, PGC2018-096446-B-C21 funded by MCIN/AEI/10.13039/501100011033 and "ERDF A way of making Europe", RYC-2016-20208 funded by MCIN/AEI/10.13039/501100011033 and "ESF Investing in your future", Grant TED2021-130358B-I00 funded by MCIN/AEI/10.13039/501100011033, FPU20/01311 funded by the Spanish Ministry of Universities.

References

[1] C. Galindo; F. Hernando; D. Ruano, *Stabilizer quantum codes from J-affine variety codes and a new Steane-like enlargement*. Quantum Inf. Process., 14 (9), 3211–3231 (2015).
[2] I. García-Marco; I. Márquez-Corbella; D. Ruano, *High dimensional affine codes whose square has a designed minimum distance*. Des. Codes Cryptogr., 88, 1653–1672 (2020).
[3] P. Gimenez; D. Ruano; R. San-José, *Saturation and vanishing ideals*. São Paulo J. Math. Sci. (2022).
[4] P. Gimenez; D. Ruano; R. San-José, *Entanglement-assisted quantum error-correcting codes from subfield subcodes of projective Reed-Solomon codes*. ArXiv 2304.08121 (2023).
[5] M. González-Sarabia; J. Martínez-Bernal; R.H. Villarreal; C.E. Vivares, *Generalized minimum distance functions*. J. Algebr. Comb., 50, 317–346 (2019).
[6] G. Lachaud, *The parameters of projective Reed-Muller codes*. Discrete Math., 81 (2), 217–221 (1990).
[7] J. Martínez-Bernal; Y. Pitones; R.H. Villarreal, *Minimum distance functions of graded ideals and Reed–Muller-type codes*. J. Pure Appl. Algebra, 221, 251–275 (2017).
[8] L. Núñez-Betancourt; Y. Pitones; R.H. Villarreal, *Footprint and minimum distance functions*. Commun. Korean Math. Soc., 33 (1), 85–101 (2018).
[9] A.B. Sørensen, *Projective Reed-Muller codes*. IEEE Trans. Inform. Theory, 37 (6), 1567–1576 (1991).

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session on *"Effective ideal theory and combinatorial techniques in commutative and non commutative rings and their applications"*

Letterplace: theory, technology, and implementation

Viktor Levandovskyy [viktor.levandovskyy@mathematik.uni-kassel.de]

Insitute of Mathematics, Kassel University, Germany

Letterplace Gröbner bases were introduced by La Scala and Levandovskyy in [1] as an alternative way for computing Gröbner bases of two-sided ideals in a free associative algebra over a field. Later it turned out that it is possible to reformulate the procedure in the form of Buchberger's style. Nevertheless, the letterplace approach led to the creation of SINGULAR:LETTERPLACE [2], a subsystem of SINGULAR, providing very rich functionality and flexibility for a practitioner in the realm of computations with associative algebras. Moreover, the letterplace way of thinking naturally addresses nonlinear difference equations, which still wait for a serious algorithmic treatment.

Keywords
Free associative algebra, Non-commutative Gröbner basis, Non-commutative computer algebra

References
[1] ROBERTO LA SCALA AND V. LEVANDOVSKYY Letterplace ideals and non-commutative Gröbner bases. *Journal of Symbolic Computation* **44**(10), 1374–1393 (2009).
[2] V. LEVANDOVSKYY, K. ABOU ZEID AND H. SCHÖNEMANN, SINGULAR:LETTERPLACE — A SINGULAR 4-3-1 Subsystem for Non-commutative Finitely Presented Algebras, `https://www.singular.uni-kl.de`, 2023.

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session on *"Effective ideal theory and combinatorial techniques in commutative and non commutative rings and their applications"*

On binomial complete intersections

Filip Jonsson Kling[1]***, Samuel Lundqvist***[1]***,***
Lisa Nicklasson[2] [filip.jonsson.kling@math.su.se]

[1] Department of Mathematics, Stockholm University, Stockholm, Sweden
[2] Department of Mathematics, University of Genova, Genoa, Italy

An artinian monomial complete intersection $(x_1^{d_1}, \ldots, x_n^{d_n})$ enjoys the following two well known properties: the set of monomials which are not divisible by $x_i^{d_i}$ for $i = 1, \ldots, n$ is a vector space basis for the corresponding quotient, and the Macaulay dual generator equals $X_1^{d_1-1} \cdots X_n^{d_n-1}$ up to a constant factor.

In this paper we argue that these characteristics should be seen as special cases of properties of complete intersections on the form

$$I = (a_1 x_1^{d_1} - b_1 m_1, \ldots, a_n x_n^{d_n} - b_n m_n),$$

where $a_i \neq 0$, and m_i is a monomial of degree d_i. Our main results are the following.

1. Associated to I there is a graph G that gives a rewriting rule transforming any element in the polynomial ring to a linear combination of monomials not divisible by $x_i^{d_i}$ for $i = 1, \ldots, n$ modulo I. In particular, the monomials not divisible by the $x_i^{d_i}$'s constitute a vector space basis for the quotient ring.

2. The coefficients of the Macaulay dual generator are monomials in the coefficients of the generators of I, and can be described algorithmically in terms of the graph G.

3. The results above require that I is a complete intersection. The radical of the resultant of I, which is a polynomial in the a_i's and b_i's, determines for which choices of coefficients I really is a complete intersection. We determine this polynomial combinatorially in terms of G with the restriction that each m_i is not a pure power of a variable. We also give a less precise description of the radical of the resultant for our general class of ideals.

The first and the third result generalize a construction for the case $d_1 = \cdots = d_n = 2$ by Harima, Wachi, and Watanabe [1], and this paper has served as the main source of inspiration for our study.

Keywords
Complete intersection, binomial ideal, Macaulay's inverse system, resultant, term-rewriting

References

[1] TADAHITO HARIMA, AKIHITO WACHI AND JUNZO WATANABE, The resultants of quadratic binomial complete intersections. *Journal of Commutative Algebra* **12**(2), 217–235 (2020).

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session on *"Effective ideal theory and combinatorial techniques in commutative and non commutative rings and their applications"*

Pinched Veronese algebras

Lisa Nicklasson[1] [nicklasson@dima.unige.it]

[1] Dipartimento di Matematica, Università di Genova, Genova, Italy

A graded k-algebra A is said to be a *Koszul algebra* if the minimal free resolution of the field k over A is linear. *Linear* in this setting means that all the maps in the resolution are represented by matrices with all nonzero entries being homogeneous of degree one. Koszul algebras were introduced by Priddy in 1970, and it turned out that this homological definition pinpoints a common property of several algebras arising naturally in different fields of mathematics, such as commutative algebra, algebraic geometry, representation theory, topology, and number theory.

We consider algebras presented as a quotient $A = R/I$ where R is a polynomial ring and I a homogeneous ideal. The algebra A is said to be *quadratic* if there is a presentation where the defining ideal I is generated in degree two. Moreover, A is *G-quadratic* if I has a Gröbner basis of polynomials of degree two. A first observation regarding Koszul algebras is that they are quadratic, and it was proved in [1] that G-quadratic algebras are Koszul. The converses does not hold in general. Aside from using Gröbner bases, one can search for a *Koszul filtration* in order to prove that an algebra is Koszul. This approach was recently applied in [6] to prove that Chow rings of matroids are Koszul.

One class of G-quadratic algebras are the Veronese subalgebras. The *d-th Veronese subalgebra* of a polynomial ring R is the subring generated by all the monomials of degree d in R. In the 1990s Peeva and Sturmfels raised the question whether the so called *pinched Veronese subalgebra*

$$k[x^3,\, x^2y,\, x^2z,\, xy^2,\, xz^2,\, y^3,\, y^2z,\, z^2y,\, z^3] \quad \text{not containing } xyz \tag{1}$$

is Koszul. This concrete question turned out difficult to answer, but the problem was eventually solved by Caviglia in 2009, [2]. Caviglia's proof uses a Gröbner deformation technique, and computer assisted steps. An alternative proof of more theoretical nature was later provided in [3]. Even though Gröbner basis techniques are present in Caviglias proof, it does not conclude that the algebra is G-quadratic. In fact is has been verified, see [5], that there is no quadratic Gröbner basis in the toric coordinates. It is not known whether there exists a linear change of coordinates under which the pinched Veronese becomes G-quadratic.

Let $\mathrm{PV}(n, d, s)$ be the pinched Veronese subalgebra of $K[x_1, \ldots, x_n]$ generated by all monomials of degree d supported in at most s variables. With this notation the example (1) is the algebra $\mathrm{PV}(3,3,2)$. In [5] it is asked for which parameters n, d, s the algebra $\mathrm{PV}(n,d,s)$ is quadratic or Koszul. We address this question in [4].

Theorem ([4])**.** *The pinched Veronese algebra* $\mathrm{PV}(n,d,s)$ *is quadratic if* $s \geq \lceil (n+1)/2 \rceil$.

As $\mathrm{PV}(n,d,s)$ is generated by monomials it can be presented as the quotient of a polynomial ring and a binomial ideal. A key observation for the proof of the above theorem is that monomials of degree d generating $\mathrm{PV}(n,d,s)$ span a 2-normal vector space, meaning that $\mathrm{PV}(n,d,s)$ contains all monomials of degree $2d$. Any algebra generated by monomials spanning a 2-normal space can be presented as the quotient by an ideal generated by binomials of degree at most three. Hence, proving that the algebras are quadratic boils down to showing that no relations of degree three are needed. When $1 < s < \lceil (n+1)/2 \rceil$ the pinched Veronese algebras $\mathrm{PV}(n,d,s)$ are in general not quadratic. The following problem remains open.

> *Are the pinched Veronese algebras* $\mathrm{PV}(n,d,s)$ *with* $s \neq 1$ *quadratic if and only if* $s \geq \lceil (n+1)/2 \rceil$*, with say a few exceptions for small values of* n, d, s*? Are they also Koszul in this case?*

Keywords
pinched Veronese algebras, Koszul algebra, G-quadratic algebras

References

[1] D. ANICK, On the homology of associative algebras, *Trans. Amer. Math. Soc.*, **296**,641–659 (1986).
[2] G. CAVIGLIA, The Pinched Veronese is Koszul, *J. Algebraic Combin.*, **30**, 539–548 (2009).
[3] G. CAVIGLIA AND A. CONCA, Koszul property of projections of the Veronese cubic surface, *Adv. in Math.*, **234**, 404–413 (2013).
[4] L. COLARTE-GÓMEZ, R. M. MIRÓ-ROIG, AND L. NICKLASSON, Monomial projections of Veronese varieties: New results and conjectures, *J. Algebra*, **626**, 82–108 (2023).
[5] A. CONCA, E. DE NEGRI, AND M. E. ROSSI, Koszul algebras and regularity, In *Commutative Algebra: Expository Papers Dedicated to David Eisenbud on the Occasion of His 65th Birthday*, 285–315. Springer New York, New York, NY (2013).
[6] M. MASTROENI AND J. MCCULLOUGH, Chow rings of matroids are Koszul, *Math. Ann.*, https://doi.org/10.1007/s00208-022-02506-5 (2022).

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session on *"Effective ideal theory and combinatorial techniques in commutative and non commutative rings and their applications"*

Almost monomial subalgebras of $\mathbb{K}[x]$ and their LAGBI bases

Victor Ufnarovski[1]***, Erik Kennerland***[1]***,***
Anna Torstensson[1] [victor.ufnarovski@math.lth.se]

[1] Lund Institute of Technology/ Centre for Mathematical Sciences, Lund, Sweden

Let $\mathbb{K}$ be an arbitrary field and A be a unital subalgebra in $\mathbb{K}[x]$. We call A **almost monomial** if it contains all monomials of sufficiently large degree. Using the terminology from [1] almost monomial subalgebras are exactly those with $\mathrm{Sp}(A) = \{0\}$. Furthermore we know from that paper that such subalgebras have the property that only the value of f and finitely many its derivatives in zero determine if $f \in A$. From that paper we also know that determining so called 0-derivations is vital in order to describe possible subalgebras of A.

In this paper we prove a conjecture about the possible structure of $0-$derivations formulated in [1]. We show also that for any two such subalgebras $A \supset B$ we can create a chain $A_1 = A \supset A_2 \cdots \supset A_n = B$ such that A_{i+1} has codimension one in A_i and can be obtained as a kernel of some $0-$derivation of A_i. This shows that the result in [2] for these type of algebras hold for any field.

One of our main tools for studying an almost monomial algebra will be a certain associated semigroup: If $f(x) = \sum a_i x^i$ is a non-zero polynomial in $\mathbb{K}[x]$ we define its **lower degree** as
$$\mathrm{ldeg}(f) = \min\{k | a_k \neq 0\}.$$
The set of all possible lower degrees
$$S_A^{(L)} = \{\mathrm{ldeg}(f) | f \in A\}$$
forms a semigroup, that we call the **lower semigroup** of A.

We show that the **multiplicity** $m(A)$ and the **Frobenius number** $F(A)$ of this semigroup are important invariants of A.

We also introduce the notion of **LAGBI** basis which is similar to a SAGBI basis, but based on ldeg of polynomials instead of ordinary degree. We describe an efficient algorithm to construct such a basis and show how to use it in order to understand the structure of A and its $0-$derivations.

Keywords
almost monomial subalgebras, LAGBI bases, 0-derivations.

References

[1] GRÖNKVIST, RODE, LEFFLER, ERIK; TORSTENSSON, ANNA; UFNAROVSKI, VICTOR, Subalgebras in $K[x]$ of small codimension. *Appl. Algebra Engrg. Comm. Comput.,* **33** 751–789. https://link.springer.com/article/10.1007/s00200-022-00573-4 (2022)

[2] E.A., GORIN Subalgebras of finite codimension. *Mathematical Notes of the Academy of Sciences of the USSR* **6**, 649–652 (1969). https://doi.org/10.1007/BF01119685

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session on *"Effective ideal theory and combinatorial techniques in commutative and non commutative rings and their applications"*

On simplification of comprehensive Gröbner systems

Yosuke Sato[1]***, Ryoya Fukasaku***[2] [ysato@rs.tus.ac.jp]

[1] Department of Applied Mathematics, Tokyo University of Science, Tokyo, Japan
[2] Department of Mathematics, Kyushu University, Fukuoka, Japan

A comprehensive Gröbner system (CGS) introduced in [14] is a powerful tool for handling a parametric ideal. Since the paper was published, several relevant researches such as [4-13,15] have been done. A first efficient algorithm is introduced in [13] based on the work of [2]. It is further improved by [3-5,9-10]. By those algorithms, we can now have practical implementations of several algorithms of computer algebra which use CGS computation such as the quantifier elimination algorithm introduced in [1].

A CGS is defined as follows, where $\bar{A} = A_1, \ldots, A_m$ are parameters and $\bar{X} = X_1, \ldots, X_n$ are main variables.

Definition 1.
Let F be a finite subset of $\mathbb{Q}[\bar{A}, \bar{X}]$ and $>$ a term order on the set of terms of $\bar{X}$. A comprehensive Gröbner system of F w.r.t. $>$ is a finite set $\mathcal{G} = \{((E_1, D_1), G_1), \ldots, ((E_s, D_s), G_s)\}$ with finite subsets E_i, D_i of $\mathbb{Q}[\bar{A}]$ and a finite subset G_i of $\mathbb{Q}[\bar{A}, \bar{X}]$ for each i such that $\{\mathbb{V}(E_i) - \mathbb{V}(D_i) | i = 1, \ldots, s\}$ is a partition of $\mathbb{C}^m$ and $G_i(\bar{a})$ becomes a Gröbner basis of the ideal $\langle F(\bar{a}) \rangle$ in $\mathbb{C}[\bar{X}]$ w.r.t. $>$ for any $\bar{a} \in \mathbb{C}^m$ which lies in $\mathbb{V}(E_i) - \mathbb{V}(D_i)$. ($G_i(\bar{a})$ and $F(\bar{a})$ denote the sets of polynomials in $\mathbb{C}[\bar{X}]$ obtained from G_i and F by specializing the parameters $\bar{A}$ with $\bar{a}$.)

In order to apply CGS computation to any algorithm, a simple representation of a CGS is indispensable for its efficient implementation. The algorithms introduced in [3-5,9-10,13] take some simplification devices into account. For example, we can have E_i, D_i such that the ideals $I_i = \langle E_i \rangle$ and $J_i = \langle D_i \rangle$ are radical ideals satisfying $I_i = I_i : J_i^\infty$ that is $\mathbb{V}(I_i)$ is the Zariski closure of $\mathbb{V}(I_i) - \mathbb{V}(J_i)$. Such a pair (E_i, D_i) has no redundancy, hence it can be considered as the simplest representation of the locally closed set $\mathbb{V}(I_i) - \mathbb{V}(J_i)$ in some sense.

For the simplification of G_i, however, non of them uses informations we can obtain from D_i.

Example. Let $F = \{(B^2-1)X+AB, A^2+B^2-1\}$ be a set of polynomials in $\mathbb{Q}[A,B,X]$. Considering A, B as the parameters and X as the main variable, the CGS of F produced by either of the algorithms of [3-5,9-10,13] contains

$$((\{A^2+B^2-1\}, \{B^2-1\}), \{(B^2-1)X+AB\}).$$

When $A^2+B^2-1=0$, $(B^2-1)X+AB = -A^2X+AB = -A(AX-B)$. If $B^2-1 \neq 0$ in addition, $A^2 = -(B^2-1) \neq 0$, hence $A \neq 0$. Therefore, we can change it to

$$((\{A^2+B^2-1\}, \{B^2-1\}), \{AX-B\})$$

by replacing the polynomial $(B^2-1)X+AB$ with a simpler polynomial $AX-B$.
Important thing is that the polynomial is actually contained in a saturation ideal, that is

$$AX - B \in \langle (B^2-1)X+AB, A^2+B^2-1\rangle : \langle B^2-1\rangle^\infty.$$

In [11], we reported that the above relation generally holds. More precisely, we introduced the following relation $\succeq^{I,J}$ and showed the following theorem holds.

Definition 2.
Let I, J are radical ideals of $\mathbb{Q}[\bar{A}]$ such that $I \supsetneq J$ and $I = I : J^\infty$. Let $f(\bar{A},\bar{X}), p(\bar{A},\bar{X})$ be polynomials in $\mathbb{Q}[\bar{A},\bar{X}]$. If there exists a polynomial $h(\bar{A}) \in \mathbb{Q}[\bar{A}]$ such that

$$\forall \bar{a} \in \mathbb{V}(I) - \mathbb{V}(J) \;\; h(\bar{a}) \neq 0 \text{ and } f(\bar{a},\bar{X}) = h(\bar{a})p(\bar{a},\bar{X}),$$

we write $f \succeq^{I,J} p$. $f \succ^{I,J} p$ denotes that $f \succeq^{I,J} p$ holds but $p \succeq^{I,J} f$ does not.

If there does not exists g such that $p \succ^{I,J} g$, p is said to be irreducible w.r.t. $\succeq^{I,J}$. An irreducible polynomial p satisfying $f \succeq^{I,J} p$ is called an irreducible form of f.

In the above example, $AX - B$ is an irreducible form of $(B^2-1)X+AB$.

Theorem.
Let f, p be polynomials in $K[\bar{A},\bar{X}]$ such that $f \succeq^{I,J} p$, then $p \in (\langle f\rangle + I) : J^\infty$.

By this theorem, for any element $f \in G$ of $((E,D),G) \in \mathcal{G}$, any irreducible form p of f w.r.t. $\succeq^{\langle E\rangle,\langle D\rangle}$ is guaranteed to belong the saturation ideal $(\langle f\rangle + \langle E\rangle) : \langle D\rangle^\infty$. Unfortunately, however, we had not obtained an algorithm to compute it at that time.

In this talk, we study the relation $\succeq^{I,J}$ in more detail, and introduce new results concerning an algorithm to compute an irreducible form of a given polynomial.

Our results are embedded in our prototype implementation on the computer algebra system SageMath [16]. Some computation data is also introduced in the talk for showing effectiveness of our results.

Keywords
Comprehensive Gröbner System, SageMath, saturation ideal

References

[1] 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.

[2] M. KALKBRENER, *On the stability of Gröbner bases under specializations.* J. Symb. Comp., Vol 24, pp. 51–58, 1997.

[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] D. KAPUR; Y. SUN; D. WANG, *An efficient algorithm for computing a comprehensive Gröbner system of a parametric polynomial system.* J. Symb. Comp., Vol. 49, pp. 27–44, 2013.

[5] 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.

[6] M. MANUBENS; A. MONTES, *Improving DISPGB algorithm using the discriminant ideal.* J. Symb. Comp., Vol. 41, pp. 1245–1263, 2006.

[7] A. MONTES, *A new algorithm for discussing Gröbner bases with parameters.* J. Symb. Comp., Vol. 33, pp. 183–208, 2002.

[8] A. MONTES, *The Gröbner cover.* Algorithms and Computation. in Mathematics, 27. Springer, Cham, 2018.

[9] K. NABESHIMA, *A speed-up of the algorithm for computing comprehensive Gröbner systems.* Proc. ISSAC 2007, pp. 299–306, ACM, 2007.

[10] K. NABESHIMA, *Stability Conditions of Monomial Bases and Comprehensive Gröbner systems.*, Lecture Notes in Computer Science, Vol. 7442, pp. 248–259, Springer, 2012.

[11] Y. SATO, *Simplification of comprehensive Gröbner systems using disequalities.* Presented in ACA2022, Gebze Technical University, Turkey, August 15-19, 2022.

[12] A. SUZUKI; Y. SATO, *An alternative approach to comprehensive Gröbner bases.* J. Symb. Comp., Vol. 36, pp. 649–667, 2003.

[13] 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.

[14] V. WEISPFENNING,*Comprehensive Gröbner bases.* J. Symb. Comp., Vol. 14, pp. 1–29, 1992.

[15] V. WEISPFENNING,*Canonical comprehensive Gröbner bases.* J. Symb. Comp., Vol. 36, pp. 669–683, 2003.

[16] *SageMath*, A free open-source mathematics software system licensed under the GPL. `https://www.sagemath.org/`

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session on *"Effective ideal theory and combinatorial techniques in commutative and non commutative rings and their applications"*

Term elimination sequence and removal of extraneous factors in two-polynomial systems

Tateaki Sasaki[1] [sasaki@math.tsukuba.ac.jp]

[1] Professor emeritus, University of Tsukuba, Tsukuba-shi, Ibaraki 305-8571, Japan

In computer algebra, two kinds of polynomial representations are used mostly. One is the recursive representation used by the resultants [4], and another is the monomial representation used by the Gröbner bases [2]. Given polynomials G and H represented as sums of monomials, the $\mathrm{Spol}(G, H)$ is defined to cancel the leading-monomials of G and H by multiplying as low-order monomials as possible to them. Similarly, treating G and H as polynomials represented recursively w.r.t. their variables, we define $\mathrm{Elim}(G, H)$ to cancel the leading-terms of G and H by multiplying as low-order terms as possible to them. Both the $\mathrm{Spol}(G, H)$ and the $\mathrm{Elim}(G, H)$ are "critical-pair"s of Knuth-Bendix [6, 3].

Let G and H be in $\mathbb{K}[x, \boldsymbol{u}]$, where $\boldsymbol{u} = (u_1, \ldots, u_n)$, with $x \succ u_i$ for any i, and let $d = \deg_x(G) \geq \deg_x(H) = e$. By $\mathrm{lcf}(F)$ for $F \in \mathbb{K}[x, \boldsymbol{u}]$, we denote the leading-coefficient of F w.r.t. the main variable x. Then, the $\mathrm{Elim}(G, H)$ is expressed as follows.

$$\mathrm{Elim}(G, H) = [\mathrm{lcf}(H)/c]G - x^{d-e}[\mathrm{lcf}(G)/c]H, \quad \text{where } c = \gcd(\mathrm{lcf}(G), \mathrm{lcf}(H)). \quad (1)$$

The Elim operation was proposed in [7], but not investigated until recently. So, we survey it briefly. The G and H in $\mathrm{Elim}(G, H)$ are called *operand* and *eliminator*, respectively. Assuming that G and H are relatively prime, we can eliminate x by computing a "Term Elimination Sequence", TES in short, as $(P_1 := G,\ P_2 := H,\ P_3 := \mathrm{Elim}(P_1, P_2),\ \ldots,\ P_k := \mathrm{Elim}(P_{k-2}, P_{k-1}))$, where $0 \neq P_k \in \mathbb{K}[\boldsymbol{u}]$. Note that $\deg_x(P_{i-1}) \geq \deg_x(P_i)$ for $\forall i > 1$. If $\deg_x(P_{i-1}) = \deg_x(P_i)$ then the TES may branch there, because we may choose P_i as the operand, hence we must compare both branches. If P_i is used as the eliminator twice or more, then we say that the TES becomes *abnormal* at the i-th element. For computing the abnormal TES, see [1] or [9]. For each element P_i, we can compute $A_i, B_i \in \mathbb{K}[x, \boldsymbol{u}]$ satisfying $A_i G + B_i H = P_i$ and *degree conditions* $\deg_x(A_k) < \deg_x(H)$ and $\deg_x(B_k) < \deg_x(G)$. Thus, TES is similar to the PRS.

The Gröbner basis is one of the most important concepts in modern computer algebra. Only one fault of it is that its computation is often quite heavy. Recently, the present speaker and his collaborators tried to improve this situation by using the TES, see a survey paper [1]. Using the recursive polynomial representation, we can eliminate x efficiently. However, this approach encounters a serious problem: the multivariate resultants obtained by this method contain pretty large *extraneous factors* mostly, and researchers could not remove the extraneous factors until recently, see [5]. In this talk, the speaker presents a new method of removing the extraneous factors contained in $R := \mathrm{resultant}(G, H)$ for obtaining the lowest-order element $\widehat{S}_2$ of the elimination ideal $\langle\{G, H\}\rangle \cap \mathbb{K}[\boldsymbol{u}]$, by using the TES of G and H.

We consider how Buchberger's method computes $\widehat{S}_2$. Employing the lexicographic monomial order, the method can obtain an $R \in \mathbb{K}[\boldsymbol{u}]$. Let $\Gamma_2 = \{E_1, E_2, \ldots, E_l\}$ be an intermediate basis when the R has just been computed. Then, Buchberger's method constructs $\mathrm{Spol}(R, E_i)$ for each E_i of Γ_2, updating R and Γ_2. Repeating this, we find $\widehat{S}_2$ eventually. We perform similar operations for the elements of $\mathrm{TES}(G, H)$, by selecting an "optimal" TES, as follows. At each branching point of TES, we first select one branch so that the last element P_k is of the lowest order. Next, if $\deg(P_{i-1}) = \deg(P_i)$ then we discard P_{i-1}. Finally, for each element P_{k-i} $(1 \le i \le k-1)$ of the optimal TES, we eliminate x by P_k with the Elim operation, and we name the resulting polynomial in $\mathbb{K}[\boldsymbol{u}]$ as P_{k+i}.

First, we compute P_{k+1}. Assuming $\deg_x(P_{k-1}) = 1$, we express P_{k-1} as $C_{1,1}(\boldsymbol{u})x + C_{1,0}(\boldsymbol{u})$, where $C_{1,1} \neq 0$. Putting $\theta_{1,1} := \gcd(C_{1,1}, P_k)$, we get $P_{k+1} \stackrel{\mathrm{def}}{=} \mathrm{Elim}(P_{k-1}, P_k) = [P_k/\theta_{1,1}]P_{k-1} - [C_{1,1}/\theta_{1,1}]\, xP_k = [P_k/\theta_{1,1}](C_{1,1}\, x + C_{1,0}) - [C_{1,1}/\theta_{1,1}]\, xP_k = [P_k/\theta_{1,1}]C_{1,0}$. Next, let us compute P_{k+2}, by expressing P_{k-2} as $C_{2,2}(\boldsymbol{u})x^2 + C_{2,1}(\boldsymbol{u})x + C_{2,0}(\boldsymbol{u})$, where $C_{2,2} \neq 0$. Putting $\theta_{2,2} := \gcd(C_{2,2}, P_k)$, we compute $P'_{k+2} \stackrel{\mathrm{def}}{=} \mathrm{Elim}(P_{k-2}, P_k) = [P_k/\theta_{2,2}](C_{2,1}\, x + C_{2,0})$. Since P'_{k+2} contains x, we apply Elim operation further. Putting $\theta_{2,1} := \gcd(C_{2,1}, P_k)$, we eliminate x^1-term of P'_{k+2}, obtaining $P_{k+2} \stackrel{\mathrm{def}}{=} \mathrm{Elim}(P'_{k+2}, P_k) = [P_k/\theta_{2,2}] \times \big([P_k/\theta_{2,1}](C_{2,1}\, x + C_{2,0}) - [C_{2,1}/\theta_{2,1}]\, xP_k\big) = [P_k/\theta_{2,2}][P_k/\theta_{2,1}]\, C_{2,0}$. We can generalize the above results easily, as follows. Let $P_{k-i} = C_{i,i}(\boldsymbol{u})x^i + C_{i,i-1}(\boldsymbol{u})x^{i-1} + \cdots + C_{i,0}(\boldsymbol{u})x^0$, where $C_{i,0} \neq 0$, then P_{k+i} is expressed as follows.

$$P_{k+i} = [P_k/\theta_{i,i}] \cdots [P_k/\theta_{i,1}]C_{i,0}, \quad \text{where } \theta_{i,j} = \gcd(C_{i,j}, P_k) \quad (i \ge j \ge 1). \tag{2}$$

Now, we impose a question: what is $\theta_{1,1}$, for example. Is it necessary?, i.e., it contains a part of $\widehat{S}_2$, or is it extraneous?, or both?. We cannot check the first case, because we do not know $\widehat{S}_2$; the possibility of this case is small because $\widehat{S}_2$ is small. Hence, we consider only the case that the $\theta_{1,1}$ is extraneous. Similarly, we assume that, for any $i \ge 2$, each $\theta_{i,j}$, $(i \ge \forall j \ge 1)$, are extraneous. Then, the amount of the extran. factors of P_k computed by P_{k-i} are bounded by $\mathrm{lcm}(\theta_{\mathrm{i,i}}, \ldots, \theta_{\mathrm{i,1}})$. Here, the Least-Common-Multiple operation is applied to avoid multiple counting of the same factors. The extraneous factors will be over-estimated, so we must check **over-removal** of extran. factors when P_k is updated.

We expect that removing extraneous factors of P_k by repeating the above method, we will be able to compute $\widehat{S}_2$; however, we have not proved it yet.

As for computing $\widehat{S}_2$, the speaker and Inaba [8] presented a very efficient method: compute $A_k, B_k \in \mathbb{K}[x, \boldsymbol{u}]$ satisfying $A_k G + B_k H = P_k$ with the degree conditions by the extended Euclidean algorithm, then $\widehat{S}_2 = P_k/C$ where $C := \gcd(\mathrm{cont}_x(A_k), \mathrm{cont}_x(B_k))$. The proof in [8] is very complicated, but the speaker found a very simple proof recently; see [1, 9]. Compared with the method in [8], the method in this talk may be more expensive, but the method shows clearly how the extraneous factors are removed.

The speaker is now working to apply the TES to three-or-more polynomial systems.

Keywords
term elimination sequence, extraneous factors, removal of extraneous factors

References

[1] T. SASAKI, A Bridge between Euclid and Buchberger (An Attempt to Enhance Gröbner Basis Algorithm by PRSs and GCDs). 28 pages, ACM Communications in Comp. Alg., 2023 (to appear).
[2] B. BUCHBERGER, Gröbner bases: an algorithmic methods in polynomial ideal theory. *Multidimensional Systems Theory*, Chap. 6. Reidel Publishing (1985).
[3] B. BUCHBERGER AND R. LOOS, Algebraic Simplification. *Computer Algebra (Computing Supplementum 4)*, Springer-Verlag, pp.11-43 (1982).
[4] D. COX, J. LITTLE AND D. O'SHEA, Ideals, Varieties, and Algorithms –An Introduction to Computational Algebraic Geometry and Commutative Algebra, Second Edition, Chap. 3 (Elimination Theory), §6, Springer-Verlag, 1997.
[5] D. KAPUR, Algebraic elimination methods. Tutorial paper to ISSAC '95. Mail to kapur@cs.albany-edu.
[6] D.E. KNUTH AND P.B. BENDIX, Simple Word Problem in Universal Algebras. *Proceedings of Conference on Comput. Problems in Abstract Algebra*, Oxford, 261-298 (1967).
[7] T. SASAKI, H. IMAI, T. ASANO AND K. SUGIHARA, *Computational Algebra and Computational Geometry* (in Japanese). Chap. 5. Iwanami Lecture Series on Applied Mathematics, Vol. 5, Iwanami Book Publishing (Japan), (1993).
[8] T. SASAKI AND D. INABA, Simple relation between the lowest-order element of ideal $\langle\{G, H\}\rangle$ and the last element of polynomial remainder sequence. *Proceedings of SYNASC 2017* (Symb. Numer. Algori. Sci. Comp.), IEEE Conf. Publ. Serv., 55-62 (2018).
[9] T. SASAKI, On the TES (Term Elimination Sequence) (mostly in Japanese, important parts in English). RIMS Kôkyûroku (Research Reports of RIMS (Research Institute of Mathematical Sciences, Kyoto Univ., Japan) (to appear).

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session on *"Effective ideal theory and combinatorial techniques in commutative and non commutative rings and their applications"*

Testing tameness of a complex polynomial map via comprehensive Gröbner systems

Shinichi Tajima[1], ***Katsusuke Nabeshima***[2] [tajima@math.tsukuba.ac.jp]

[1] Graduate School of Science and Technology, Niigata University, 8050, Ikarashi 2-no-cho, Nishi-ku Niigata, Japan
[2]Department of Applied Mathematics, Tokyo University of Science, 1-3, Kagurazaka, Tokyo, Japan

Let $f : \mathbb{C}^n \longrightarrow \mathbb{C}$ be a polynomial map. In [1], S. A. Broughton considered the following problem:

How can we build up the topology of $f^{-1}(a), a \in \mathbb{C}$, from a knowledge of the local Milnor fibrations around critical points of f?

He introduced the following notion.

Definition A polynomial $f : \mathbb{C}^n \longrightarrow \mathbb{C}$ is called *tame* if the following holds:

There is a $\delta > 0$ such that the set $\{x \in \mathbb{C}^n \mid |\frac{\partial f}{\partial x_1}(x)|^2 + |\frac{\partial f}{\partial x_2}(x)|^2 + \cdots + |\frac{\partial f}{\partial x_n}(x)|^2 \geq \delta\}$ is compact.

Assume that f is a polynomial with only isolated critical points.

Let $x_0 \in \mathbb{C}^n$ be a critical point of f. Let $\mathcal{O}_{\mathbb{C}^n,x_0}$ be the stalk at x_0 of the sheaf $\mathcal{O}_{\mathbb{C}^n}$ of holomorphic functions. Let J_{x_0} denote the Jacobi ideal $(\frac{\partial f}{\partial x_1}, \frac{\partial f}{\partial x_2}, \ldots, \frac{\partial f}{\partial x_n})_{x_0}$ in the local ring $\mathcal{O}_{\mathbb{C}^n,x_0}$ and let μ_{x_0} denote the Milnor number at x_0 of f defined to be the colength $\dim_{\mathbb{C}}(\mathcal{O}_{\mathbb{C}^n,x_0}/J_{x_0})$ of the ideal J_{x_0}.

The total Milnor number μ of f is defined to be the sum of all $\mu_{x_0}, x_0 \in \mathbb{C}^n$. For $a \in \mathbb{C}$, let μ^a denote the sum of all the local Milnor number on $f^{-1}(a)$.

One of the main results of S. A. Broughton presented in [1] is the following.

Theorem Let f be a polynomial with only isolated critical points. Assume that f is tame. Then, the hypersurface $f^{-1}(a), a \in \mathbb{C}$ has the homotopy type of a bouquet of $\mu - \mu^a$ spheres of dimension $n - 1$.

Recall that the topology of $f^{-1}(a)$ can not be, in general, determined by the set of critical values of f.

The tameness of a polynomial is a fundamental concept in the study of topology of polynomial map. Note also that the concept of tameness was generalized by several authors and has been applied, for instance, by A. Douai [4], C. Sabbah [8] and M. Schulze [9] in their study of Gauss-Manin connections.

We consider in this note a method for testing tameness of a polynomial map. We give, based on results of S. A. Broughton published in [2], an effective algorithm for testing tameness of polynomial maps. Main ingredient of our approach is the theory of comprehensive Gröbner systems [5, 6, 7]. Furthermore, we show that our method can be extended to handle parametric cases [3]. As an application, we give an algorithm for computing the homotopy type of the hypersurfaces $f^{-1}(a), a \in \mathbb{C}$ of a tame polynomial.

Keywords
Tameness, comprehensive Gröbner system, local Milnor fibration

References

[1] S. A. Broughton, On the topology of polynomial hypersurfaces, *Proc. Sympos. in Pure Math.* **40**, 167-178, (1983)
[2] S. A. Broughton, Milnor numbers and the topology of polynomial hypersurfaces. *Invent. Math.* **92**, 217-241, (1988)
[3] P. Cassou-Noguès, Sur la généralisation d'un théorème de Koushnirenko. *Compositio Math.* **103**, 95-121, (1996)
[4] A. Douai, Très bonnes bases du réseau du Brieskorn d'un polynôme modéré. *Bull. de la S. M. F* **127**, 255-287, (1999)
[5] D. Kapur, Y. Sun, and D. Wang, An efficient algorithm for computing a comprehensive Gröbner system of a parametric polynomial system. *J. Symbolic Computation.* **49**, 74–44, (2013)
[6] A. Montes, *The Groebner Cover*, Springer 2019.
[7] K. Nabeshima, A speed-up of the algorithm for computing comprehensive Gröbner systems. In *ISSAC 2007*, 299-306, ACM New York, 2007
[8] C. Sabbah, Hypergeometric period for a tame polynomial. *C. R. Acad. Sci. Paris* **328**, 603-608, (1999)
[9] M. Schulze, Good bases for tame polynomials. *J. Symbolic Computation.* **39**, 103-126, (2005)

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session on *"Effective ideal theory and combinatorial techniques in commutative and non commutative rings and their applications"*

Primary decomposition via algebraic local cohomology with tag variables

Katsusuke Nabeshima[1], ***Shinichi Tajima***[2] [nabeshima@rs.tus.ac.jp]

[1] Department of Applied Mathematics, Tokyo University of Science, Japan
[2] Graduate School of Science and Technology, Niigata University, Japan

In this talk, we introduce how to compute a primary decomposition of an ideal via algebraic local cohomology classes. In particular, the method has a good feature that the main part of the method consists of linear algebra techniques.
Let K be a subfield of the field $\mathbb{C}$ of complex numbers and x the abbreviation of n variables $x_1, \ldots, x_n$. Let $H^n_{[O]}(K[x])$ denote the set of algebraic local cohomology classes supported at the origin O with coefficients in K, defined by
$H^n_{[O]}(K[x]) := \lim_{k\to\infty} \mathrm{Ext}^n_{K[x]}(K[x]/\langle x_1, \ldots, x_n\rangle^k, K[x])$
where $\langle x_1, \ldots, x_n\rangle$ is the maximal ideal generated by $x_1, \ldots, x_n$.
We represent an algebraic local cohomology class by a finite sum of the form $\sum c_\lambda \begin{bmatrix} 1 \\ x^\lambda \end{bmatrix}$ where $c_\lambda \in K$, $\lambda \in \mathbb{Z}^n_{\geq 1}$ and $[\ ]$ is the Grothendieck symbol. The multiplication by x^β is defined as

$$x^\beta * \begin{bmatrix} 1 \\ x^\lambda \end{bmatrix} = \begin{cases} \begin{bmatrix} 1 \\ x^{\lambda-\beta} \end{bmatrix} & \lambda_i > \beta_i,\ \ i = 1, 2, \ldots, n, \\ 0 & \text{otherwise}, \end{cases}$$

where $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$, $\lambda = (\lambda_1, \ldots, \lambda_n) \in \mathbb{Z}^n_{\geq 1}$.
Fix a term ordering $\succ$ on $\mathbb{Z}^n_{\geq 1}$. For a given algebraic local cohomology class of the form $\psi = c_\lambda \begin{bmatrix} 1 \\ x^\lambda \end{bmatrix} + \sum_{\lambda\succ\beta} c_\beta \begin{bmatrix} 1 \\ x^\beta \end{bmatrix}$ $(c_\lambda, c_\beta \in K)$, we call $\begin{bmatrix} 1 \\ x^\lambda \end{bmatrix}$ the *head term*, c_λ the *head coefficient*, λ the *head exponent*, $\begin{bmatrix} 1 \\ x^\beta \end{bmatrix}$ the *lower terms* and β the *lower exponents*. We denote the head term by $\mathrm{ht}(\psi)$, the head coefficient by $\mathrm{hc}(\psi)$ and the head exponent by $\mathrm{hex}(\psi)$. Furthermore, we denote the set of terms of ψ as $\mathrm{Term}(\psi)$, the set of lower terms of ψ as $\mathrm{LL}(\psi) = \left\{ \begin{bmatrix} 1 \\ x^\kappa \end{bmatrix} \in \mathrm{Term}(\psi) \middle| \begin{bmatrix} 1 \\ x^\kappa \end{bmatrix} \neq \mathrm{ht}(\psi) \right\}$ and the set of exponents of $\mathrm{Term}(\psi)$ as $\mathrm{Expo}(\mathrm{Term}(\psi)) = \left\{ \lambda \in \mathbb{Z}^n_{\geq 1} \middle| \begin{bmatrix} 1 \\ x^\lambda \end{bmatrix} \in \mathrm{Term}(\psi) \right\}$. For a finite subset $\Psi \subset H^n_{[O]}(K[x])$, $\mathrm{ht}(\Psi) = \{\mathrm{ht}(\psi) | \psi \in \Psi\}$ and $\mathrm{LL}(\Psi) = \bigcup_{\psi\in\Psi} \mathrm{LL}(\psi)$. Let $\lambda \in \mathbb{Z}^n_{\geq 1}$ and $\Phi \subset \mathbb{Z}^n_{\geq 1}$. For each

$1 \leq i \leq n$, we call $\lambda + \boldsymbol{e}_i$ a neighbor of λ where $\boldsymbol{e}_i$ is the ith unit vector. We define the neighbors of Φ as Neighbor(Φ), i.e. $\mathrm{Neighbor}(\Phi) = \{\gamma + \boldsymbol{e}_i | \gamma \in \Phi, i = 1, \ldots, n\}$. Set $\Lambda = \mathrm{Neighbor}(\Phi) \backslash \Phi$ and $\mathrm{Cor}(\Phi) = \Lambda \backslash \left(\bigcup_{\alpha \in \Lambda} \left\{ \beta \in \Lambda | \exists \gamma \in \mathbb{Z}^n_{\geq 0} \backslash \{(0,..,0)\} \text{ s.t. } \beta = \alpha + \gamma \right\} \right)$. An element of $\mathrm{Cor}(\Phi)$ is called a *corner* of Φ.
Let F be a set of s polynomials $f_1, f_2, \ldots, f_s$ in $K[x]$ such that $\mathbb{V}_K(F) \cap X = \{O\}$ where $\mathbb{V}_K(F) = \{a \in K^n | f_i(a) = 0, 1 \leq i \leq s\}$ and X is an open neighborhood of the origin O of K^n. We define a set H_F to be the set of algebraic local cohomology classes associated to F in $H^n_{[O]}(K[x])$ that are annihilated by the ideal generated by F, where $H_F = \{\psi \in H^n_{[O]}(K[x]) \mid f_1 * \psi = f_2 * \psi = \cdots = f_s * \psi = 0\}$. Since $\mathbb{V}_K(F) \cap X = \{O\}$, H_F is a finite dimensional vector space. In our previous works [3,4,5], we introduced and implemented algorithms for computing bases of the vector space H_F. Note that these algorithms mainly consist of linear algebra techniques.

Definition 1. *Let $\succ$ be a term order on $\mathbb{Z}^n_{\geq 0}$.*
(1) The term order $\succ$ is called global if $\alpha \succ (0,0,\ldots,0)$ for all $\alpha \neq (0,0,\ldots,0)$.
(2) The term order $\succ$ is called local if $(0,0,\ldots,0) \succ \alpha$ for all $\alpha \neq (0,0,\ldots,0)$.
(3) The inverse order $\succ^{-1}$ of $\succ$ is defined by $\alpha \succ \beta \iff \beta \succ^{-1} \alpha$ where $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$.

Note that if a term order $\succ$ is local, then the inverse term order $\succ^{-1}$ is global.

Definition 2. *Let us fix a (global or local) term order on $\mathbb{Z}^n_{\geq 0}$. Let Ψ_F be a basis of the vector space H_F such that for all $\psi \in \Psi_F$, $\mathrm{hc}(\psi) = 1$, $\mathrm{ht}(\psi) \notin \mathrm{ht}(\Psi_F \backslash \{\psi\})$ and $\mathrm{ht}(\psi) \notin \mathrm{LL}(\Psi_F)$. Then, the basis is called a reduced basis of H_F w.r.t. $\succ$.*

Definition 3. *Let $\succ$ be a local term order on $\mathbb{Z}^n_{\geq 1}$ and Ψ a subset of $H^n_{[O]}(K[x])$ such that an element forms $\begin{bmatrix} 1 \\ x^\lambda \end{bmatrix} + \sum_{\lambda \succ \tau} c_{(\lambda,\gamma)} \begin{bmatrix} 1 \\ x^\tau \end{bmatrix}$ where $c_{(\lambda,\gamma)} \in K$ and $\tau \in \mathbb{Z}^n_{\geq 1}$. For $\gamma = (\gamma_1, \ldots, \gamma_n) \in \mathbb{Z}^n_{\geq 1}$, the transfer GB_Ψ is defined by the following*

$$\begin{cases} \mathrm{GB}_\Psi(\gamma) = x^{\gamma - 1} - \displaystyle\sum_{\kappa \in \mathrm{hex}(\psi)} c_{(\kappa,\gamma)} x^{\kappa - 1} & \text{in } K[x], \quad \text{if } \gamma \in \mathrm{Expo}(\mathrm{LL}(\Psi)), \\ \mathrm{GB}_\Psi(\gamma) = x^{\gamma - 1} & \text{in } K[x], \quad \text{if } \gamma \notin \mathrm{Expo}(\mathrm{LL}(\Psi)), \end{cases}$$

where $\kappa = (\kappa_1, \ldots, \kappa_n) \in \mathbb{Z}^n_{\geq 1}$, $\gamma - 1 = (\gamma_1 - 1, \ldots, \gamma_n - 1)$, $\kappa - 1 = (\kappa_1 - 1, \ldots, \kappa_n - 1)$. For a subset $\Phi \subset \mathbb{Z}^n_{\geq 1}$, the set $\mathrm{GB}_\Psi(\Phi)$ is also defined by $\mathrm{GB}_\Psi(\Phi) = \{\mathrm{GB}_\Psi(\gamma) | \gamma \in \Phi\}$.

Since $\mathbb{V}_K(F) \cap X = \{O\}$, $\langle F \rangle$ has $\mathfrak{q}_O$ with $\sqrt{\mathfrak{q}_O} = \langle x_1, \ldots, x_n \rangle$ as a primary components of $\langle F \rangle$. The primary component can be directly obtaind from a reduced basis of H_F w.r.t. a local term order $\succ$, as follows.

Theorem 4. *Let F be a finite subset in $K[x]$ with $\mathbb{V}_K(F) \cap X = \{O\}$, Ψ a reduced basis of the vector space H_F w.r.t. a local term order $\succ$ in $H^n_{[O]}(K[x])$ and $\Phi = \mathrm{Cor}(\mathrm{Expo}(\mathrm{ht}(\Psi)))$ in $\mathbb{Z}^n_{\geq 1}$. Then, $\mathrm{GB}_\Psi(\Phi)$ is the reduced Gröbner basis of $\mathfrak{q}_O$ w.r.t. the global term order $\succ^{-1}$ in $K[x]$.*

Let I be a zero-dimensional ideal and $\mathfrak{q} \cap \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_t$ a minimal primary decomposition of I with the prime ideal $\sqrt{\mathfrak{q}} = \mathfrak{p}$. Next, we consider how to compute a primary component of $\mathfrak{q}$ via algebraic local cohomolgy classes. Note that it is reported that algorithms, published in [1,2,3], for computing a prime decomposition of the radical $\sqrt{I}$ are much faster than those for computing primary decomposition of a polynomial ideal I in $K[X]$. One can utilized the algorithms for computing a prime component of $\sqrt{I}$.

In order to facilitate the discussion easily, let $\{p_1, \ldots, p_\ell\} \subset K[x]$ be the reduced Gröbner basis of a prime ideal $\mathfrak{p}$ w.r.t. a global term order $\succ_x$ and $\mathfrak{q} \subset K[x]$ a primary ideal with $\sqrt{\mathfrak{q}} = \mathfrak{p}$ and $\mathfrak{p} \neq \langle 1 \rangle$. Set $p_1 - z_1, p_2 - z_2, \ldots, p_\ell - z_\ell$ where $z_1, \ldots, z_n$ are *tag variables*. That is, we regard $(K[x]/\mathfrak{p})[p_1, \ldots, p_\ell]$ as $(K[x]/\mathfrak{p})[z_1, \ldots, z_\ell]$ as follows.

Lemma 5. *Let $\succ_{x \cup z}$ be a block term order in $\mathbb{Z}_{\geq 0}^{n+\ell}$ with $\succ_x$ and $x \gg \{z_1, \ldots, z_\ell\}$ and G a Gröbner basis of the ideal $\langle p_1 - z_1, p_2 - z_2, \ldots, p_\ell - z_\ell \rangle$ w.r.t. $\succ_{x \cup z}$. For $f \in \mathfrak{q}$, let $g = \overline{f}^G$ be the remainder of g on division by G. Then,*
(i) $g(z_1, \ldots, z_\ell) \in (K[x]/\mathfrak{p})[z_1, \ldots, z_\ell]$, and
(ii) $f = g(p_1, \ldots, p_\ell)$ is an expression of f as a polynomial in $p_1, \ldots, p_\ell$.

Lemma 6. *Let $I = \langle f_1, \ldots, f_s \rangle$ be a zero-dimensional ideal, $\mathfrak{q}$ a primary component of I and $\sqrt{\mathfrak{q}} = \mathfrak{p} = \langle p_1, \ldots, p_\ell \rangle$. Let $\succ_{x \cup z}$ be a block term order with $\succ_x$ and $x \gg \{z_1, \ldots, z_\ell\}$ and G a Gröbner basis of the ideal $\langle p_1 - z_1, p_2 - z_2, \ldots, p_\ell - z_\ell \rangle$ w.r.t. $\succ_{x \cup z}$. Set $F' = \left\{\overline{f_1}^G, \overline{f_2}^G, \ldots, \overline{f_s}^G\right\}$ in $(K[x]/\mathfrak{p})[z_1, \ldots, z_\ell]$. Then, $\mathbb{V}_{K[x]/\mathfrak{p}}(F') \cap X = \{O\}$ where X is an open neighborhood of the origin O of $(K[x]/\mathfrak{p})^\ell$.*

Proposition 7. *Using the same notation as in Lemma 6, a set $H_{F'}$ of algebraic local cohomology classes in $H^\ell_{[O]}((K[x]/\mathfrak{p})[z_1, \ldots, z_\ell])$, is a finite dimensional vector space. Furthermore, there exist algorithms for computing a basis of the vector space.*

Theorem 8. *Using the same notation as in Lemma 6, let B be a basis of $\mathfrak{q}$ in $K[x]$ and B' a basis of a primary component $\mathfrak{q}'$ of the ideal $\langle F' \rangle$ in $(K[x]/\mathfrak{p})[z_1, \ldots, z_\ell]$ where $\sqrt{\mathfrak{q}} = \langle p_1, p_2, \ldots, p_\ell \rangle$ in $K[x]$ and $\sqrt{\mathfrak{q}'} = \langle z_1, z_2, \ldots, z_\ell \rangle$ in $(K[x]/\mathfrak{p})[z_1, \ldots, z_\ell]$. Then, $\mathfrak{q} = \langle \{g(p_1, \ldots, p_\ell) \in K[x] \mid g(z_1, \ldots, z_\ell) \in B' \subset (K[x]/\mathfrak{p})[z_1, \ldots, z_\ell]\} \rangle$.*

The primary component $\mathfrak{q}' \subset (K[x]/\mathfrak{p})[z_1, \ldots, z_\ell]$ can be obtained by utilizing Theorem 4. Thus, by utilizing the theorem above, it is possible to obtain the primary component $\mathfrak{q} \subset K[x]$.

Keywords
Primary decomposition, algebraic local cohomology, Gröbner basis

References
[1] T. Aoyama and M. Noro, Modular algorithms for computing minimal associated primes and radicals of polynomial ideals. In *ISSAC2018*, 31-38, ACM (2018)
[2] T. Kawazoe and M. Noro, Algorithms for computing a primary ideal decomposition without producing intermediate redundant components, *J. Symbolic Computation*, **46**, 1158–1172, (2011)
[3] K. Nabeshima and S. Tajima, On efficient algorithms for computing parametric local cohomology classes associated with semi-quasihomogeneous singularities and standard bases. In *ISSAC2014*, 351–358, ACM (2014)
[4] K. Nabeshima and S. Tajima. Algebraic local cohomology with parameters and parametric standard bases for zero-dimensional ideals. *J. Symbolic Computation* **82**, 91–122, (2017)
[5] S. Tajima, Y. Nakamura and K. Nabeshima, Standard bases and algebraic local cohomology for zero dimensional ideals. *Advanced Studies in Pure Mathematics* **56**, 341-361, (2009)

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session on *"Effective ideal theory and combinatorial techniques in commutative and non commutative rings and their applications"'*

A Gröbner basis as a combination of congruence closures

Deepak Kapur[1] [kapur@unm.edu]

[1] The University of New Mexico, Albuquerque, USA

A novel perspective on the Groebner basis algorithm for polynomial ideals over the integers [1] is presented. The approach utilizes a congruence closure algorithm, incorporating associative-commutative (AC) function symbols with identities, to handle ground equations. Specifically, two congruence closure algorithms are combined: one for the AC function symbol '$+$' with 0 as the identity, and another for the AC symbol '$*$' with 1 as the identity. Constants are treated as shared symbols [2].
Terms (expressions) constructed using these symbols are transformed into an equivalent sum-of-products form through the distributivity property. By employing purification and introducing new symbols, two separate subsystems of equations are generated: one using '$+$' and another using '$*$'. Canonical rewrite systems are independently derived from each subsystem and subsequently combined by overlapping pairs of rules that share a constant from both the '$+$' and '$*$' subsystems.
Each subsystem can be analyzed independently using termination orderings that extend a common ordering on constant symbols. The distributivity property between '$*$' and '$+$' as well as the zero property of multiplication are accounted for by employing a new critical pair/superposition construction among terms belonging to different symbols but sharing a constant.
This alternative perspective offers significant flexibility and enables modular and simplified proofs of correctness. Termination orderings on polynomials are not required to be admissible on the original symbols, resulting in the generation of "weird" Groebner bases. While reduction (simplification) on polynomials in the original symbols may not be terminating, it remains confluent. "Weird" canonical forms can be associated with elements of the quotient ring defined by a polynomial ideal.
This view of the Groebner basis algorithm for polynomial ideals over the integers deviates significantly from other approaches in the literature, including the popular one that treats it as an instance of the Knuth-Bendix completion procedure proposed by Kandri-Rody, Kapur, and Winkler in 1989 [3], especially when generalized to AC symbols and/or richer equational theories [5]. Instead, it aligns more closely with regarding the polynomial equivalence problem modulo an ideal as a word problem over a finitely presented commutative ring with unity, as proposed by Kandri-Rody, Kapur, and Narendran in 1985 [4].

Keywords
Groebner bases, polynomials over integers, congruence closure algorithm, associative-commutative

References

[1] A. KANDRI-RODY; D. KAPUR, *An Algorithm for Computing the Gröbner Basis of a Polynomial Ideal over an Euclidean Ring*. Journal *Symbolic Computation,* 6 (1), August 1988, 37-57.
[2] D. KAPUR, *Modularity and Combination of Associative Commutative Congruence Closure Algorithms enriched with Semantic Properties*. *Logical Methods in Computer Science*, 19(1) (2023).
[3]A. KANDRI-RODY; D. KAPUR; F. WINKLER, *Knuth-Bendix Procedure and Buchberger Algorithm – A Synthesis*. Proceedings *ACM-SIGSAM 1989 International Symposium on Symbolic and Algebraic Computation - ISSAC '89*, Portland, OR, July 1989, 55-67.
[4] A. KANDRI-RODY; D. KAPUR; P. NARENDRAN, *An Ideal-Theoretic Approach for Word Problems and Unification Problems over Commutative Algebras*. Proceedings *First International Conference on Rewriting Techniques and Applications (RTA-85)*, Dijon, France (eds. Jouannaud and Musser), May 1985, Springer LNCS 202, 345-364.
[5] C. MARCHE, *Normalized rewriting: An alternative to rewriting modulo a set of equations*. Journal *Symbolic Computation.*, 21(3):253–288, 1996.

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session on *"Algebraic and Algorithmic Aspects of Differential and Integral Operators (AADIOS)"*

Doctrine specific ur-algorithms

Mohamed Barakat[1] [mohamed.barakat@uni-siegen.de]

[1] University of Siegen

Various constructions of categories have a universal property expressing the freeness/initiality of the construction within a specific categorical doctrine. Expressed in an algorithmic framework, it turns out that this universal property is in a certain sense a doctrine-specific "ur-algorithm" from which various known categorical constructions/algorithms can be derived in a purely computational way. This can be viewed as a categorical version of the Curry-Howard correspondence to extract programs from proofs.

Keywords
category theory, doctrines, left adjoints

References
[1] SEBASTIAN POSUR, On free abelian categories for theorem proving. *Journal of Pure and Applied Algebra* **226**(7), Paper No. 106994, 19 (2022).

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session on *“Algebraic and Algorithmic Aspects of Differential and Integral Operators (AADIOS)”*

The most general theory of one-sided fractions

V. V. Bavula[1] [v.bavula@sheffield.ac.uk]

[1] School of Mathematics and Statistics, University of Sheffield, Sheffield, UK

Ore’s method of localizations is an example of a theory of one-sided fractions. The aim of the talk is to introduce the most general theory of one-sided fractions based on the papers [1] and [2].

Keywords
localization, one-sided fraction, Ore set

References

[1] V. V. BAVULA, Localizable sets and the localization of a ring at a localizable set, *J. Algebra*, **610** (2022), no. 15, 38–75.
[2] V. V. BAVULA, Localizations of a ring at localizable sets, their groups of units and saturations, *Math. Comp. Sci.*, **16** (2022), no. 1, Paper No. 10, 15 pp.

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session on *"Algebraic and Algorithmic Aspects of Differential and Integral Operators (AADIOS)"*

The Newton-Puiseux algorithm and effective algebraic series

Manfred Buchacher[1] [manfredi.buchacher@gmail.com]

[1] RICAM, Austrian Academy of Sciences, Linz, Austria

Given a polynomial $p(x, y)$ in two variables x and y over an algebraically closed field $\mathbb{K}$ of characteristic zero, the classical Newton-Puiseux algorithm [2] determines the first terms of a series ϕ in x over $\mathbb{K}$ that solves $p(x, \phi) = 0$. Finding a series solution of a polynomial equation is one and the most apparent aspect of the algorithm. However, it also permits to encode algebraic series by a finite amount of data and to effectively compute with them on the level of these encodings. While this is well-known for univariate algebraic series, this is not the case for algebraic series that are multivariate. We explain how to do effective arithmetic with multivariate algebraic series and complement the discussion of the Newton-Puiseux algorithm for (multivariate, not necessarily bivariate) polynomials over a field of characteristic zero in [3]. We also show that the convex hull of the support of an algebraic series is a polyhedral set and explain how the Newton-Puiseux algorithm and an effective equality test for algebraic series can be used to compute its vertices and bounded faces.

Keywords
Newton-Puiseux algorithm, algebraic series, effective arithmetic, supports of series

References

[1] MANFRED BUCHACHER, *The Newton-Puiseux Algorithm and Effective Algebraic Series.* arXiv:2209.00875, 2022.
[2] EGBERT BRIESKORN, HORST KNÖRRER, *Plane Algebraic Curves.* Springer Science & Business Media, 2012.
[3] JOHN MCDONALD, *Fiber polytopes and fractional power series.* Journal of Pure and Applied Algebra **104** (2), 213–233, 1995.

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session on *“Algebraic and Algorithmic Aspects of Differential and Integral Operators (AADIOS)”*

New dimension polynomials and invariants of inversive difference-differential field extensions

Alexander Levin [levin@cua.edu]

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

We introduce a new type of reduction in the ring of inversive difference-differential polynomials and use the corresponding technique of autoreduced sets to prove the existence and outline a method of computation of dimension polynomials of a new type associated with finitely generated inversive difference-differential field extensions. We show that the obtained dimension polynomials (which are numerical polynomials in three variables) carry more difference-differential birational invariants than previously known univariate and bivariate difference-differential dimension polynomials (see, for example, [1, Section 6.7 and Chapter 7], [2] and [3]). We describe these invariants and show how they can be applied to the equivalence problem for systems of algebraic difference-differential equations.

Keywords
Difference-differential field, autoreduced set, dimension polynomial

References
[1] M. V. KONDRATEVA, A. B. LEVIN, A. V. MIKHALEV, AND E. V. PANKRATEV, *Differential and Difference Dimension Polynomials*. Kluwer Acad. Publ., 1999.
[2] A. B. LEVIN, Reduced Gröbner bases, free difference-differential modules and difference-differential dimension polynomials. *J. Symbolic Comput.*, **30** (2000), 357–382.
[3] M. ZHOU AND F. WINKLER, Computing difference-differential dimension polynomials by relative Gröbner bases in difference-differential modules. *J. Symbolic Comput.*, **43** (2008), 726–745.

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session on *"Algebraic and Algorithmic Aspects of Differential and Integral Operators (AADIOS)"*

Computation of Koszul homology and application to involutivity of partial differential systems

Cyrille Chenavier[1]***, Thomas Cluzeau***[1]***, Alban Quadrat***[2] [cyrille.chenavier@unilim.fr]

[1] XLIM, Université de Limoges, Limoges, France
[2] Institut de mathématiques de Jussieu-Paris rive gauche, Université Sorbonne, Paris, France

This talk will be a presentation of the paper [1]. The formal integrability of systems of partial differential equations plays a fundamental role in different analysis and synthesis problems for both linear and nonlinear differential control systems. Following Spencer's theory, to test the formal integrability of a system of partial differential equations, we must study when the symbol of the system, namely, the top-order part of the linearization of the system, is 2-acyclic or involutive, i.e., when certain Spencer cohomology groups vanish. Using the well-known fact that Spencer cohomology is dual to Koszul homology and symbolic computation methods, we show how to effectively compute the homology modules defined by the so-called Koszul complex of a finitely presented module over a commutative polynomial ring. These results are implemented using the OREMORPHISMS package. We then use these results to effectively characterize 2-acyclicity and involutivity of the symbol of a system of partial differential equations. Finally, we show explicit computations on different examples.

Keywords
formal integrability, involutivity, Koszul complex

References
[1] C. CHENAVIER; T. CLUZEAU; A. QUADRAT, *Computation of Koszul homology and application to involutivity of partial differential systems*. IFAC Symposium on System Structure and Control (SSSC 2022).

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session on *"Algebraic and Algorithmic Aspects of Differential and Integral Operators (AADIOS)"*

A semi-decision procedure for proving operator statements

Clemens Hofstadler[1]***, Clemens G. Raab***[2]***,***
Georg Regensburger[1] [chofstadler@mathematik.uni-kassel.de]

[1] Institute of Mathematics, University of Kassel, Kassel, Germany
[2] Institute for Algebra, Johannes Kepler University, Linz, Austria

Linear operators play a fundamental role in various mathematical contexts, appearing as ring elements (e.g., in C^*-Algebras), as (rectangular) matrices, or as vector space and module homomorphisms. In this talk, we present a recently developed algebraic framework [1] for proving first-order statements about linear operators by computations with noncommutative polynomials. Furthermore, we present our new SAGEMATH package `operator_gb` [2], which offers functionality for automatising such computations. We aim to provide a practical understanding of our approach and the software through examples, including recent work [3], while also explaining the completeness of the method in the sense that it allows to find algebraic proofs for every true first-order operator statement. Our main result is a semi-decision procedure that allows to automatically prove operator statements phrased within first-order logic based on a single computation with noncommutative polynomials.

Keywords
linear operators, first-order statements, noncommutative polynomials

References

[1] C. HOFSTADLER, C. G. RAAB, AND G. REGENSBURGER, Universal truth of operator statements via ideal membership. *arXiv preprint*, arXiv:2212.11662 (2022).
[2] K. BERNAUER, C. HOFSTADLER, AND G. REGENSBURGER, How to automatise proofs of operator statements: Moore-Penrose inverse – a case study. *arXiv preprint*, arXiv:2305.09448 (2023).
[3] D. S. CVETKOVIĆ-ILIĆ, C. HOFSTADLER, J. HOSSEIN POOR, J. MILOŠEVIĆ, C. G. RAAB, AND G. REGENSBURGER, Algebraic proof methods for identities of matrices and operators: improvements of Hartwig's triple reverse order law. *Applied Mathematics and Computation* **409**: 126357 (2021).

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session on *"Algebraic and Algorithmic Aspects of Differential and Integral Operators (AADIOS)"*

A differential algebraic approach of systems theory

Sette Diop[1] [sette.diop@cnrs.fr]

[1] Université Paris-Saclay, CNRS, CentraleSupélec, Laboratoire des signaux et systèmes, Gif sur Yvette, France

Differential algebraic geometry (and differential algebra) [1,2] was earlier recognized as particularly adapted as a language for the description of some of the systems theory problems. See the pioneering works by Jean-François Pommaret [3] and Michel Fliess [4]. In the latter paper the notion of invertibility, which was long studied in the control literature, was given a better clarification. And in the [5] differential algebraic elimination theory was invoked as, not only a better description of questions in the control literature, but a constructive answer, too. One of the fundamental notions of systems theory, that of observability, was also given a differential algebraic geometry description which clarified many aspects of that questions [6]. This contribution is a tentative comprehensive expose of differential algebraic geometry known answers to some of the systems theory questions. The latter include previously mentioned ones, and notions of invariants, structural issues, and constructivity.

Keywords
Systems theory, Nonlinear systems, Differential algebraic geometry

References
[1] J. F. RITT, *Differential Algebra*. American Mathematical Society, Providence, RI, 1950.
[2] E. R. KOLCHIN, *Differential Algebra and Algebraic Groups*. Academic Press, New York, 1973.
[3] J. F. POMMARET, *Differential Galois Theory*. Gordon and Breach, New York, 1983.
[4] M. FLIESS, A note on the invertibility of nonlinear input-output differential systems. *Systems Control Lett.* **4**, 17–32 (1986).
[5] S. DIOP, Elimination in control theory. *Math. Control Signals Systems* **8**(2), 147–151 (1991).
[6] S. DIOP, From the geometry to the algebra of nonlinear observability. In *Contemporary Trends in Nonlinear Geometric Control Theory and its Applications*, A. Anzaldo-Meneses, B. Bonnard, J. P. Gauthier and F. Monroy-Perez (eds.), 305–345. World Scientific Publishing Co., Singapore, 2002.

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session on *"Algebraic and Algorithmic Aspects of Differential and Integral Operators (AADIOS)"*

Hypergeometric creative telescoping

Shaoshi Chen[1]***, Hao Du***[3]***, Hui Huang***[4]***, Ziming Li***[1,2] [schen@amss.ac.cn]

[duhao@bupt.edu.cn, ymgao@amss.ac.cn, huanghui@dlut.edu.cn, zmli@mmrc.iss.ac.cn]

[1]KLMM, Academy of Mathematics and Systems Science, Chinese Academy of Sciences,Beijing 100190, China
[2]School of Mathematical Sciences, University of Chinese Academy of Sciences, Beijing 100049, China
[3]School of Sciences, Beijing University of Posts and Telecommunications, Beijing 100876, China
[4]School of Mathematical Sciences, Dalian University of Technology, Dalian, Liaoning, 116024, China

In this talk, we adapt the theory of normal and special polynomials from symbolic integration to the summation setting, and then built up a general framework embracing both the shift and the q-shift cases. In the context of this general framework, we are able to unify the methods of creative telescoping for hypergeometric terms and q-hypergeometric terms using reductions. These two cases will be split up only when it is really necessary. This way instantly reveals the intrinsic difference between the shift and the q-shift cases, and hopefully, provides us more insights about the more general cases. This is joint work with Hao Du, Hui Huang and Ziming Li.

Keywords
Creative Telescoping, q-Hypergeometric Term, Reduction, Symbolic Summation

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session on *"Algebraic and Algorithmic Aspects of Differential and Integral Operators (AADIOS)"*

Crossed homomorphisms and Cartier-Kostant-Milnor-Moore theorem for difference Hopf algebras

Li Guo[1], ***Yunnan Li***[2], ***Yunhe Sheng***[3], ***Rong Tang***[3] [liguo@rutgers.edu]

[1] Department of Mathematics and Computer Science, Rutgers University, Newark, NJ 07102, USA
[2] School of Mathematics and Information Science, Guangzhou University, Guangzhou 510006, China
[3] Department of Mathematics, Jilin University, Changchun 130012, Jilin, China

The celebrated Milnor-Moore theorem and the more general Cartier-Kostant-Milnor-Moore theorem establish close relationships of a connected and a pointed cocommutative Hopf algebra with its Lie algebra of primitive elements and its group of group-like elements. Crossed homomorphisms for Lie algebras, groups and Hopf algebras have been studied extensively, first from a cohomological perspective and then more broadly, with an important case given by difference operators. In this talk we show that the relationship among the different algebraic structures captured in the Milnor-Moore theorem can be strengthened to include crossed homomorphisms and differenece operators. We give a graph characterization of Hopf algebra crossed homomorphisms which are also compatible with the Milnor-Moore relation. We further investigate derived actions from crossed homomorphisms on groups, Lie algebras and Hopf algebras, and establish their relationship. Finally we obtain a Cartier-Kostant-Milnor-Moore type structure theorem for pointed cocommutative difference Hopf algebras. Examples and classifications of difference operators are also provided for several Hopf algebras.

Keywords
crossed homomorphism, difference operator, Hopf algebra, Lie algebra, Milnor-Moore theorem, Cartier-Kostant-Milnor-Moore theorem

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session on *"Algebraic and Algorithmic Aspects of Differential and Integral Operators (AADIOS)"*

Approximate symmetries and conservation laws and their applications to PDEs

Alexei Cheviakov[1] [shevyakov@math.usask.ca]

[1] Department of Mathematics and Statistics, University of Saskatchewan, Saskatoon, SK, Canada

Many nonlinear PDE models that arise in applications are in some sense "close" to integrable PDEs or other equations with rich analytical structure but lack such structure themselves. For PDE models with small parameter(s), one may be interested in finding symmetries, conserved quantities, and solutions that hold approximately [1,2], up to higher order terms in the small parameter(s). I will discuss approaches to the systematic construction of such approximate quantities and approximate solutions, their mathematical aspects, usefulness and relevance in the physical context [3], and examples of symbolic computer algebra-based computation [4] of these objects. This is a joint work with Mahmood Tarayrah and Zhengzheng Yang.

Keywords
Nonlinear PDEs, Apprioximate symmetries, Apprioximate conservation laws, Symbolic computation

References
[1] V. A. BAIKOV, R. K. GAZIZOV, AND N. H. IBRAGIMOV, Approximate groups of transformations. *Differentsial'nye Uravneniya* **29**(10), 1712–1732 (1993).
[2] W. FUSHCHICH AND W. SHTELEN, On approximate symmetry and approximate solutions of the nonlinear wave equation with a small parameter. *Journal of Physics A: Mathematical and General* **22**(18), L887 (1989).
[3] R. TARAYRAH, BRIAN PITZEL, A. F. CHEVIAKOV, Two approximate symmetry frameworks for nonlinear partial differential equations with a small parameter: comparisons, relations, approximate solutions. *European Journal of Applied Mathematics* 1–29 (2022).
[4] A. F. CHEVIAKOV, GeM software package for computation of symmetries and conservation laws of differential equations. *Computer Physics Communications* **176**(1), 48–61 (2007).

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session on *"Algebraic and Algorithmic Aspects of Differential and Integral Operators (AADIOS)"*

Difference-differential polynomials in SageMath

Antonio Jiménez-Pastor[1] [ajpa@cs.aau.dk]

[1] DEIS, Aalborg University, Aalborg, Denmark

In this talk we are going to present `dalgebra`, a new module developed for SageMath [7] focused on the description of the structures and elements necessary to work in the fields of Differential or Difference Algebra.

A differential ring [6] is a pair (R, ∂) where R is a ring and ∂ a derivation over R. Similarly, a difference ring is a pair (R, σ) where now σ is a ring homomorphism. From these rings we can build difference/differential extensions, we can state respectively summation or integration problems, we can try to solve difference or differential systems, etc. In particular, there is a particular extension of particular interest for us: the ring of difference/differential polynomials.

There are many problems in both the differential and the difference world, in some cases even equivalent problems: as an example we can consider the Symbolic Integration problem [3] and Symbolic Summation problem [8]. We found that a generic software to work with these objects is not easy to find. There are implementations for linear operators (both with differences and derivation) in SageMath (`ore_algebra` [4]), in Maple (`OreTools` [1]), and in Mathematica (`HolonomicFunctions` [5]). We can also find an implementation of differential polynomials (not difference) in the Maple package `DifferentialAlgebra` [2].

This is the reason we decided to implement a new package in SageMath [7], an open source Computer Algebra software based on Python. This new package `dalgebra` provides a simple framework to define difference and differential ring and even a combination of the two. It also implements the difference and differential polynomials. This is a great starting point to implement further algorithms in the world of difference and differential algebra.

The package `dalgebra` is publicly available on Github[1] and is under active development, adding more features and improving the user interface. In this talk we will present the main features of `dalgebra`, including but not being limited to how we handle differential rings, how to set up a system of such equations and how to manipulate differential polynomials.

Keywords
difference algebra, differential algebra, SageMath, linear operators

[1] `https://github.com/Antonio-JP/dalgebra`

References

[1] S.A. ABRAMOV, H.Q. LE, AND Z. LI, Univariate ore polynomial rings in computer algebra. *Journal of Mathematical Sciences* **131**(5), 5885–5903 (2005).
[2] F. BOULIER, The Blad libraries. (2004).
[3] M. BRONSTREIN, *Symbolic Integration I: Transcendental Functions*. Springer, Berlin, 1997.
[4] M. KAUERS, M. JAROSCHEK, AND F. JOHANSSON, Ore polynomials in Sage. *Computer Algebra and Polynomials* LNCS **8942**, 105–125 (2014).
[5] C. KOUTSHCAN, Holonomic functions in Mathematica. *ACM Communications in Computer Algebra* **47**(4), 179–182 (2013).
[6] J.F. RITT, *Differential Algebra*. AMS, 1950.
[7] THE SAGE DEVELOPERS, SageMath, the Sage Mathematics Software System (Version 9.8), , 2023, https://www.sagemath.org.
[8] C. SCHNEIDER, A difference ring theory for symbolic summation. *Hournal of Symbolic Computation* **72**, 82–0127 (2016).

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session on *“Algebraic and Algorithmic Aspects of Differential and Integral Operators (AADIOS)”*

Towards an effective integro-differential elimination theory

***Thomas Cluzeau*[1]*, Camille Pinto*[2]*, Alban Quadrat*[2]** [camille.pinto@inria.fr]

[1] Université de Limoges, XLIM, Limoges, France
[2] Inria Paris, IMJ–PRG, Paris, France

Algebraic analysis is a mathematical theory which studies linear systems of ordinary or partial differential equations using rings of partial differential operators, module theory, homological algebra etc. Within this approach, a linear functional system yields a finitely presented left module over a non commutative polynomial ring of functional operators. Structural properties and equivalences of linear systems can be intrinsically reformulated within module theory and homological algebra. A classic environment in algebra is a noetherian ring with finitely generated modules. An example is the Weyl algebra $\mathbb{A}_1$: the ring of differential operators with polynomial coefficients in one variable (coefficient living in the commutative field $\mathbb{k}$). But some algebras are not noetherian, such as the algebra of entire functions, or the algebra of polynomial in an infinity of variable.

Our team research is currently interested in studying rings of integro-differential operators. The use of this rings allows one to algebraize elementary calculus by combining the differential operator, the indefinite integral and the evaluation at the initial time t_0. $\mathbb{I}_1$ usually denotes the ring of integro-differential operators in one variable with polynomial coefficients. It can be define by: « the smallest $\mathbb{k}$-algebra containing t (the operator define by the product with the elementary polynomial t), ∂ (the differential operator), and I (the integral operator) ».
Bavula worked on this subject recently (see [1]) and proved that $\mathbb{I}_1$ was not noetherian. Nonetheless, Bavula also proved that $\mathbb{I}_1$ was a coherent algebra. That means that all finitely generated sub-module of $\mathbb{I}_1$ is finitely presented. Adding a condition on sub-modules offsets the non-notherianity of $\mathbb{I}_1$ and allows us to do calculus. Yet, Bavula gave a theorical argument to say that $\mathbb{I}_1$ is coherent. We would like to make this proof effective and be able to actually make calculus in $\mathbb{I}_1$ with a computer machine.

Keywords
Integro-differential operator, Annihilator, Coherence

References
[1] V. V. BAVULA, Title. *Journal of Pure and Applied Algebra* **217**(3), 495–529 (2013).

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session on *"Algebraic and Algorithmic Aspects of Differential and Integral Operators (AADIOS)"*

Symbolic solution of differential equations

Franz Winkler[1] [franz.winkler@risc.jku.at]

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

We present the algebro-geometric method for computing explicit formula solutions for algebraic differential equations (ADEs), as described in [1]. An algebraic differential equation is a polynomial relation between a function, some of its partial derivatives, and the variables in which the function is defined. Regarding all these quantities as unrelated variables, we get an algebraic solution hypersurface; i.e., a hypersurface on which the solutions are to be found. Parametrizations of the solution hypersurface are closely related to solutions of the ADE.

This approach is relatively well understood for rational, algebraic, and power series solutions of single algebraic ordinary differential equations (AODEs). First steps are taken towards a generalization to other types of solutions and to partial differential equations.

Keywords
algebraic ODEs, symbolic solution, parametrization

References

[1] S. FALKENSTEINER, J.J. MITTERAMSKOGLER, J.R. SENDRA, F. WINKLER, The Algebro-Geometric Method: Solving Algebraic Differential Equations by Parametrization. *Bulletin (New Series) of the American Mathematical Society* **60**(1), 85–122 (2023).

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session on *“Algebraic and Algorithmic Aspects of Differential and Integral Operators (AADIOS)”*

Rational solutions of first-order algebraic ordinary difference equations

***Thieu N. Vo*[1], <u>*Yi Zhang*</u>[2]** [Yi.Zhang03@xjtlu.edu.cn]

[1] Faculty of Mathematics and Statistics, Ton Duc Thang University, Ho Chi Minh City, Vietnam
[2] Department of Foundational Mathematics, School of Mathematics and Physics,
Xi’an Jiaotong-Liverpool University, Suzhou, China

An algebraic ordinary difference equation (AOΔE) is a difference equation of the form

$$F(x, y(x), y(x+1), \cdots, y(x+m)) = 0,$$

where F is a nonzero polynomial in $x, y(x), y(x+1), \cdots, y(x+m)$ with coefficients in an algebraically closed field $\mathbb{K}$ of characteristic zero, and $m \in \mathbb{N}$. We say that an AOΔE is *autonomous* if the independent variable x does not appear in it explicitly. For computational purpose, we may choose $\mathbb{K} = \bar{\mathbb{Q}}$, the field of algebraic numbers. AOΔEs naturally appear from various problems, such as symbolic summation [2], factorization of linear difference operators [1], analysis of time or space complexity of computer programs with recursive calls [3]. Thus, to determine (closed form) solutions of a given AOΔE is a fundamental problem in difference algebra and is of general interest.

We are mainly interested in rational solutions of first-order AOΔEs. In [3], Feng, Gao and Huang proposed an algorithm for computing a rational solution for a first-order autonomous AOΔE provided that a bound for the degree of the rational solution is given. They also pointed out that they could not bound the degrees of rational solutions through the parametrization technique because the difference version of Theorem 3.7 in [2] is not always true (see Example 4.1 in [3]). We overcome this missing part and present an algorithm for computing such a degree bound, and thus derive a complete algorithm for computing corresponding rational solutions.

Keywords
algebraic ordinary difference equations; strong rational general solutions; parametrization; separable difference equation; resultant theory; algorithms

References
[1] M. BRONSTEIN; M. PETKOVŠEK, *An introduction to pseudo-linear algebra*. *Theoretical Computer Science*, 157:3–33, 1996.
[2] R. FENG; X. S. GAO, *A polynomial time algorithm for finding rational general solutions*

of first order autonomous odes. *Journal of Symbolic Computation*, 41(7):739–762, 2006.
[3] R. FENG; X. S. GAO; Z. HUANG, *Rational solutions of ordinary difference equations*. *Journal of Symbolic Computation*, , 43(10):746–763, 2008.
[4] M. PETKOVŠEK; H. S. WILF; D. ZEILBERGER, $A = B$. A K Peters Ltd., Wellesley, MA, 1996.
[5] O. SHKARAVSKA; M. VAN EEKELEN, *Polynomial solutions of algebraic difference equations and homogeneous symmetric polynomials*. *Journal of Symbolic Computation*, 103:22–45, 2021.

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session on *"Algebraic and Algorithmic Aspects of Differential and Integral Operators (AADIOS)"*

On an interplay of computer algebra and ring theory

Viktor Levandovskyy [viktor.levandovskyy@mathematik.uni-kassel.de]

Insitute of Mathematics, Kassel University, Germany

Many concepts from the ring theory are complicated or even infeasible for an algorithmic treatment. However, when algorithmizable, they often offer serious advances for applications of computer algebra. Being interested in non-commutative algebras, I will address Gelfand-Kirillov dimension and Ore localization of algebras and modules as well as generalized torsion, and discuss several important applications to problems arising in systems of linear functional equations. Many of the topics above have been supported by implementation in SINGULAR:PLURAL [1], a subsystem of SINGULAR for treating PBW algebras (a.k.a G-algebras) and providing vast functionality for modules over such algebras.

Keywords
Non-commutative computer algebra, Non-commutative Gröbner basis, Gelfand-Kirillov dimension, Ore localization

References
[1] G.-M. GREUEL, V. LEVANDOVSKYY, A. MOTSAK AND H. SCHÖNEMANN, SINGULAR:LETTERPLACE — A SINGULAR 4-3-1 Subsystem for Non-commutative Polynomial Algebras, https://www.singular.uni-kl.de, 2023.

Applications of Computer Algebra – ACA 2023
Warsaw, Poland, | July 17-21, 2023
Session on *"Algebraic and Algorithmic Aspects of Differential and Integral Operators (AADIOS)"*

An abelian ambient category for behaviors in algebraic systems theory

Sebastian Posur[1] [sebastian.posur@uni-muenster.de]

[1] University of Münster, Faculty of Mathematics and Computer Science, Münster, Germany

In the algebraic analysis approach to systems theory, systems are modeled as solution sets of finitely many linear equations over a ring, usually a ring of differential operators. These solutions are taken within some fixed module, usually a module whose elements may be interpreted as trajectories. Willems coined the term *behavior* for such solution sets [1]. Whenever our ring is noetherian and our fixed module is an injective cogenerator, a good notion of an abelian ambient category for behaviors is known in algebraic systems theory: namely the opposite category of finitely presented modules over our ring. In that good case, intrinsic features of behaviors, like being controllable or autonomous, translate into intrinsic features of finitely presented modules, like being torsion-free or torsion.

We propose a setup for algebraic systems theory that also works for an arbitrary fixed module over an arbitrary ring [2]. This setup is based on functor categories instead of module categories. This functorial setup overcomes some deficiencies that arise within the module theoretic approach, like behaviors not being isomorphic in situations where they clearly should be isomorphic. We provide an example study case with delay-differential systems.

Keywords
Algebraic systems theory, delay-differential systems, module-behavior duality, abelian categories, finitely presented functors

References

[1] JAN C. WILLEMS, *Paradigms and puzzles in the theory of dynamical systems*. IEEE Trans. Automat. Control, 36(3):259–294, 1991.
[2] S. POSUR, *An abelian ambient category for behaviors in algebraic systems theory*. arXiv, https://arxiv.org/abs/2303.02636, 2023.

SPONSORS