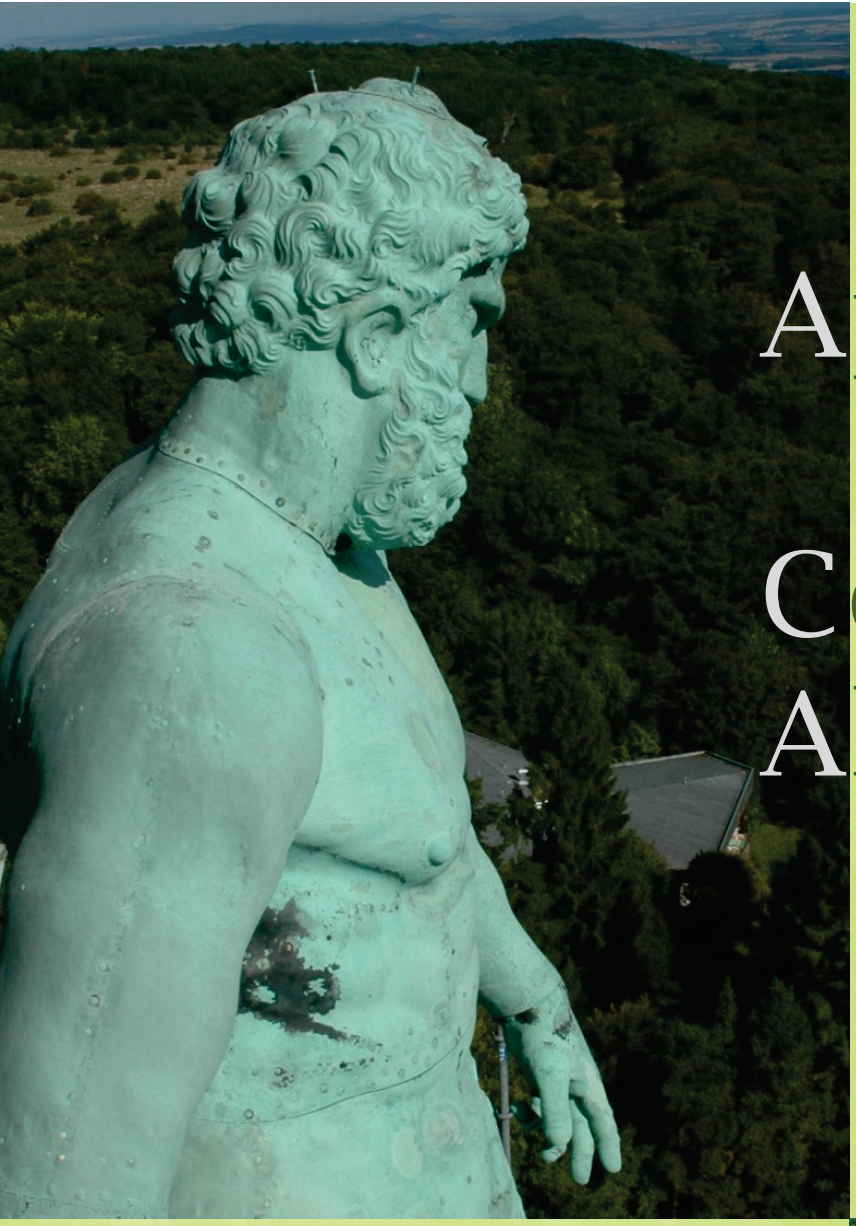


22nd Conference on Applications of Computer Algebra

ACA 2016
Kassel (Germany)
August 1st – 4th

Chairs
Wolfram Koepf and Werner Seiler (general)
Georg Regensburger
Winfried Neun
Michael Wester
(program)

Advisory Committee:
Eugenio Roanes-Lozano
Stanly Steinberg
Michael Wester

Contact:
aca2016@mathematik.uni-kassel.de

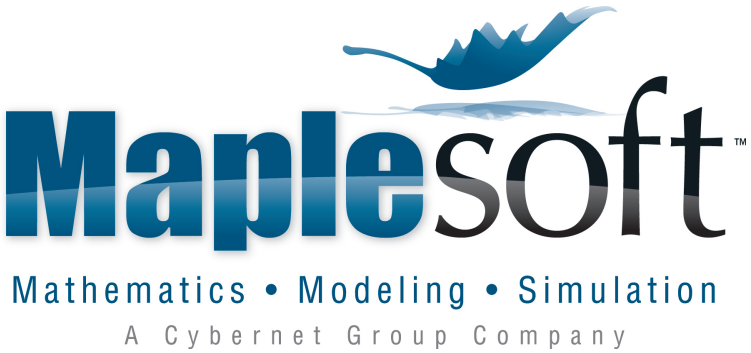
Deadline for submissions:
March 31st, 2016
submission of session proposals
May 29th, 2016
submission of talks

Notification of acceptance:
July 13th, 2016

http://www.mathematik.uni-kassel.de/ACA2016

Contents

Sponsors


Maplesoft™
Mathematics • Modeling • Simulation
A Cybernet Group Company


ADDITIVE
SOFT- & HARDWARE FÜR TECHNIK & WISSENSCHAFT


DFG
Deutsche
Forschungsgemeinschaft

Schedule

Sessions

S1	Computer Algebra for Modeling in Science and Engineering
S2	Computer Algebra in Education
S3	Human-Computer Algebra Interaction
S4	Applied and Computational Algebraic Topology
S5	Difference Computer Algebra and its Applications
S6	Computer Algebra for Dynamical Systems and Celestial Mechanics
S7	Information Services for Mathematical Software, Models, and Research Data
S8	Algebraic and Algorithmic Aspects of Differential and Integral Operator Session
S9	Automated Theorem Proving in Dynamic Geometry: Current Achievements
S10	Computer Algebra in Coding Theory and Cryptography
S11	SC-Square: Symbolic Computation and Satisfiability Checking
S12	General Session

Monday

Monday Part 1

	Room 1409	Room 1403	Room 2404	Room 1245
09:00 – 09:30	Registration			
09:30 – 10:00				
10:00 – 10:30	Opening			
10:30 – 11:00		S5 C. Fürst and G. Landsmann: Bases for Modules of Difference-Operators by Gröbner Reduction	S9 P. Quaresma: Intelligent Geometry + Dynamic Geometry	
11:00 – 11:30		S5 V.P. Gerdt, Yu.A. Blinkov and K.B. Marinov: Difference algebra aided discretization of quasilinear evolution equations	S9 A. Wassermann: sketchometry: a sketching tool for geometry	
11:30 – 12:00		S5 A. Levin: Difference Dimension Quasi-polynomials	S9 E. Roanes-Lozano: A constructive approach to the cuadrics of revolution and their equations using the DGS GeoGebra	
12:00 – 12:30		S5 C.M. Yuan: Binomial partial difference ideals	S9 Th. Dana-Picard and N. Zehavi: Managing the constraints of technology for an automated study of envelopes	
12:30 – 13:00			S9 Round table discussion	
13:00 – 13:30	Lunch Break			
13:30 – 14:00				

Monday Part 2

	Room 1409	Room 1403	Room 2404	Room 1245
14:00 – 14:30	Plenary Talk 1 Room 1409 D. Jeffrey: Computer Algebra Systems and the Lambert W Function			
14:30 – 15:00				
15:00 – 15:30	Break			
15:30 – 16:00	S8 W. M. Seiler: Algebraic Theory of Linear Partial Differential Algebraic Equations	S10 Y. Peretz: On multivariable asymmetric public-key cryptography based on simultaneous algebraic Riccati equations over finite fields	S9 B. Parisse: About Giac's Gröbner basis and ideal elimination computation	S7 W. Sperber: Information services for mathematical research data
16:00 – 16:30	S8 M. A. Barkatou and M. Jaroschek: Desingularization of First Order Linear Difference Systems with Rational Function Coefficients	S10 I. Márquez-Corbella and R. Pellikaan: Is it hard to retrieve an error-correcting pair?	S9 J. Davenport: What does `without loss of generality' mean?	S7 H. Chrapary and W. Neun: The swMATH service for mathematical software - state of the art and perspectives
16:30 – 17:00	S8 G. Grasegger, N.T. Vo and F. Winkler: Deciding Rational Solvability of First-Order Algebraic Ordinary Differential Equations	S10 P. Utomo and R. Makarim: Solving the Binary Puzzle	S9 T. Sturm: Towards higher-degree quantifier elimination by virtual substitution	S7 H.-G. Gräbe: The *SymbolicData* Project -- a Community Driven Project for the CA Community
17:00 – 17:30	S8 A. Levin: Difference-Differential Dimension Polynomials and their Invariants	S10 S. T. Dougherty, J. Rifà and M. Villanueva: Generalized hadamard Additive Codes	S9 Round table discussion	S7 A. Heinle: Benchmarks for and Quality Evaluation of CAS
17:30 – 18:00	S8 D. Robertz: Thomas Decomposition and Nonlinear Control Systems	S10 A. Fotue Tabue, E. Martínez-Moro and C. Mouaha: Galois Theory for Linear Codes		S7 Round table discussion
18:00 – 18:30	S8 G. H. E. Duchamp, H. N. Minh and N. Q. Hoan: Polylogarithms at the multi-indices of non-positive integers	S10 I. Márquez-Corbella and E. Martíinez-Moro: Betti Numbers and Generalized Hamming Weights		
18:30 – 19:00	Poster			

Tuesday

Tuesday Part 1

	Room 1409	Room 1403	Room 2404	Room 1245
09:00 – 09:30	Plenary Talk 2 Room 1409 T. Sturm: Real Problems over the Reals: From Complete Elimination Procedures to Subtropical Decisions			
09:30 – 10:00				
10:00 – 10:30	Break			
10:30 – 11:00	S8 J. H. Poor, C. G. Raab and G. Regensburger: Tensor reduction systems for operator algebras and normal forms	S1 H. Sarafian: App. of Computer Algebra System and the Mean-Value Theory for Evaluating Electrostatic Potential and its Associated Field for Nontrivial Configurations	S2 E. Varbanova and M. Durcheva: Developing Competences in Higher Mathematics in a CAS Supported Learning Environment	
11:00 – 11:30	S8 C. G. Raab and G. Regensburger: Generalized integro-differential algebra from an operator point of view	S1 A. Bilek, M. Beldi, T. Cherfi, S. Djebali and S. Larbi: Experimental and Finite Elements Stress Analysis of a Double Edge Notched Specimen	S2 J. Weitendorf: Improving mathematical competences by using modern technology	
11:30 – 12:00	S8 V. V. Bavula: Classical left regular left quotient ring of a ring and its semisimplicity criteria	S1 S. Zouaoui, H. Djebouri, A. Bilek and K. Mohammedi: Modelling and Simulation of Solid Particle Sidementation in an Incompressible Newtonian Fluid	S2 M. Durcheva and E. Varbanova: Applications of CAS in the Teaching and Learning of Discrete Mathematics	
12:00 – 12:30	S8 V. Levandovskyy: Computer Algebraic Analysis: Achievements, Perspectives and Directions (first part)	S1 S. Takato, J. A. Vallejo and M. Kaneko: Interfacing KetCindy and CASs, and its Applications to Scientific Problems Modeling	S2 R. Oldenburg: A Transparent Rule Based CAS to support Formalization of Knowledge	
12:30 – 13:00	S8 C. Schilli and V. Levandovskyy: The purity filtration of modules over Auslander regular rings	S1 T. Mylläri, A. Mylläri, A. Anckar and G. Högnäs: On the Visualization of Random Fibonacci-Padovan Sequences	S2 H.-D. Janetzko: The GUI CATO -- how natural usage of CAS with CATO modified the mathematical lectures and the interface itself	
13:00 – 13:30	Lunch Break			
13:30 – 14:00				

Tuesday Part 2

	Room 1409	Room 1403	Room 2404	Room 1245
14:00 – 14:30	Sponsor Talk 1 Room 1409 S. Szurmant: What's New in Mathematica?			
14:30 – 15:00				
15:00 – 15:30	Break			
15:30 – 16:00	S6 H. Errami, V. Gerdt, D. Grigoriev, M. Kosta, O. Radulescu, T. Sturm and A. Weber: A Case Study on the Parametric Occurrence of Multiple Steady States	S3 C. Bright, V. Ganesh, A. Heinle, I. Kotsireas, S. Nejati and K. Czarnecki: *MathCheck2*: Combining SAT and CAS	S2 S. Takato, A. McAndrew and M. Kaneko: Collaborative Use of KeTCindy and Free CASs for Making Materials	
16:00 – 16:30	S6 C. Chiralt, A. Ferragut, A. Gasull and P. Vindel: Quantitative analysis of competition models	S3 J. van der Hoeven and F. Poulain: Conservative conversion between LATEX and TEXMACS	S2 W. Wojas and J. Krupa: Visualization of simplex method with Mathematica	
16:30 – 17:00	S6 N. Vasilyev and V. Duzhin: Greedy trajectories of Plancherel processes on two dimensional Young and Schur graphs	S3 A. Kohlhase: Math Web Search Interfaces and the Generation Gap of Mathematicians	S2 Z. Kovács: Real-time animated dynamic geometry in the classrooms by using fast Gröbner basis computations	
17:00 – 17:30	S6 A. Mylläri, V. Orlov, A. Chernin and T. Mylläri: Symbolic Dynamics, Mixing and Entropy in the Three-Body Problem	S3 M. Minimair: Collaborative Computer Algebra Shell	S2 W. Wojas and J. Krupa: Familiarizing students with definition of Lebesgue integral - examples of calculation directly from its definition using Mathematica	
17:30 – 18:00	S6 Y. Tang: Global dynamics of Planar Quintic Quasi--homogeneous Polynomial Differential Systems	S3 M. Kohlhase: FrameIT: Serious Math Games from Modular Math Ontologies	S2 Th. Dana-Picard and D. Zeitoun: A framework for an ICT-based study of parametric integrals	
18:00 – 18:30		ACA Business Meeting		
18:30 – 19:00				

Wednesday

Wednesday Part 1

	Room 1409	Room 1403	Room 2404	Room 1245
09:00 – 09:30	S6 J.C. Artes, P. De Maesschalck, F. Dumortier, C. Herssens and J. Llibre: P4 and desingularization of vector fields in the plane	S4 M. Fetzer: Computing Betti numbers of Veronese subrings with Pommaret bases	S5 P. Amodio, Yu.A. Blinkov, V.P. Gerdt and R. La Scala: Gröbner basis driven construction of a new s-consistent difference approximation to Navier-Stokes equations	
09:30 – 10:00	S6 N. Kruff: Local invariant sets of analytic vector fields	S4 C. Alemán, F. Cappelli and P. Real: Some computational elements of fractal topology based on HSF structures	S5 E. Amzallag and R. Gustavson: Order Bounds for a Difference Decomposition Algorithm	
10:00 – 10:30	S6 C. Schilli, E. Zerz and V. Levandovskyy: Invariant varieties for rational control systems	S4 A. Romero, J. Rubio and F. Sergeraert: An implementation of effective homotopy of fibrations	S5 D. Robertz: Maple packages for the analysis of linear systems of partial difference equations and applications	
10:30 – 11:00	S6 J. Llibre, C. Pantazi and S. Walcher: Elementary and Darboux first integrals for planar polynomial vector fields	S4 J. González, B. Gutiérrez and S. Yuzvinsky: Motion planning of robot arms with combinatorial restrictions	S5 A.A. Kytmanov and A.P. Lyapin: On Computing Rational Generating Function of a Solution to the Cauchy Problem of Difference Equation	
11:00 – 11:30	S6 J. Torregrosa: Limit cycles in planar polynomial systems	S4 F. Diaz del Rio, D. Onchis and P. Real: Computing a new topological feature for grey-level 2D digital images: the topological hole tree	S5 M. Wibmer: Computing difference algebraic relations among solutions of linear differential equations	
11:30 – 12:00	Lunch Break			
12:00 – 12:30				
12:30 – 13:00				

Wednesday Part 2

13:00 – 13:30	Conference Excursion
13:30 – 14:00	
14:00 – 14:30	
14:30 – 15:00	
15:00 – 15:30	
15:30 – 16:00	
16:00 – 16:30	
16:30 – 17:00	
17:00 – 17:30	
17:30 – 18:00	
18:00 – 18:30	
18:30 – 19:00	Conference Dinner
19:00 –	

Thursday

Thursday Part 1

	Room 1409	Room 1403	Room 2404	Room 1245
09:00 – 09:30	Plenary Talk 3 Room 1409 P. Real: Exploring a Homotopy Approach to the Science of Data: Huge Scenarios, Topological Scintigraphy and Flagellate Structures			
09:30 – 10:00				
10:00 – 10:30	S8 E. Farrington and E. Previato: Symbolic Computation for Rankin-Cohen Differential Algebras. Klein curve as a case study.	Break		
10:30 – 11:00	S8 A. Heinle and V. Levandovskyy: Computation of all Factorizations in Certain Non-Commutative Rings	S11 E. Abraham, J. Abbott, B. Becker, A. M. Bigatti, M. Brain, B. Buchberger, A. Cimatti, J. H. Davenport, M. England, P. Fontaine, S. Forrest, A. Griggio, D. Kroening, W. M. Seiler and T. Sturm: SC^2: Satisfiability Checking meets Symbolic Computation	S1 R. Kragler: Symbolic Contour Integration in Mathematica (Part 2): Some Special Topics to be Investigated	S12 M. Albert: Computation of Hilbert Schemes
11:00 – 11:30	S8 J. Hoffmann and V. Levandovskyy: Ore localization, associated torsion and algorithms		S1 A. Prokopenya: Motion of a Swinging Atwood's Machine: Simulation and Analysis	S12 A. Hashemi: Noether Normalization and Involutive Bases
11:30 – 12:00	S8 J. Nüßle: Local Closure of Ore Algebras	S11 M. Brain: Satisfiability Modulo Theories: Where We Are, How We Got Here, and Where We Could Go Next	S1 T. Telksnys, Z. Navickas and M. Ragulskis: Construction of Analytical Solutions to Nonlinear Evolution Equations Using the Generalized Differential Operator Method	S12 D.D. Tcheutia: Divided-difference equation and three-term recurrence relations of some systems of bivariate q-orthogonal polynomials
12:00 – 12:30	S8 N. Kruff and V. Levandovskyy: Ore localization with applications in D-module theory	S11 S. Forrest: Integration of a SAT Solver into Maple	S1 A. Siluszyk: On Degenerate Central Configurations in the N-Body Problem	S12 D.D. Tcheutia, Y. Guemo Teffo, M. Foupouagnigni, E. Godoy and I. Area: Linear partial divided-difference equation satisfied by multivariate orthogonal polynomials on quadratic lattices
12:30 – 13:00	S8 V. Levandovskyy: Computer Algebraic Analysis: Achievements, Perspectives and Directions (second part)	S11 J. Abbott, A. M. Bigatti and L. Robbiano: Implicitization with Gröbner Bases: the well known algorithm and algorithms which work	S1 M.Zh. Minglibayev, A.N. Prokopenya, G.M. Mayemerova and Zh.U. Imanova: Secular Perturbations in the Two-Planetary Three-Body Problem with the Masses Varying Anisotropically with Different Rates	S12 M. Gerling: Efficient computation of the bivariate chromatic polynomial for special graphs

Thursday Part 2

	Room 1409	Room 1403	Room 2404	Room 1245
13:00 – 13:30	Lunch Break			
13:30 – 14:00				
14:00 – 14:30	Sponsor Talk 2 Room 1409 J. Gerhard: What's New in Maple 2016?			
14:30 – 15:00				
15:00 – 15:30	Break			
15:30 – 16:00	S6 C.J. Christopher and W.M.A. Hussein: A Geometric Approach for Invariant Algebraic Curves in 2D Lotka Volterra Systems I	S11 J. Abbott: Symbolic Computation: give and take for SC2		
16:00 – 16:30	S6 C.J. Christopher and W.M.A. Hussein: A Geometric Approach for Invariant Algebraic Curves in 2D Lotka Volterra Systems II	S11 Round table discussion		
16:30 – 17:00	S6 W.M. Seiler: A Dynamical Systems Approach to Singularities of Ordinary Differential Equations			
17:00 – 17:30	S6 M. Seiß: Singular Initial Value Problems for Quasi-Linear Ordinary Differential Equations			
17:30 – 18:00				
18:00 – 18:30				
18:30 – 19:00				

Plenary Talks

Computer Algebra Systems and the Lambert W Function

David Jeffrey
www.apmaths.uwo.ca/~djeffrey/

Abstract: I have worked on many aspects of computer algebra systems, mostly in conjunction with either Soft Warehouse (Derive) or Maplesoft (Maple). One particular project has touched many of the challenges that system developers face: the implementation of the Lambert W function. In this talk, I shall present some of the interesting properties of W, and use them to discuss the various challenges that our favourite systems continue to grapple with. Some examples of such challenges are branch cuts, simplification, numerical evaluation, integration.

Real Problems over the Reals: From Complete Elimination Procedures to Subtropical Decisions

Thomas Sturm
www.loria.fr/~tsturm/

Abstract: Effective quantifier elimination procedures for first-order theories provide a powerful tool for generically solving a wide range of problems based on logical specifications. In contrast to general first-order provers, quantifier elimination procedures are based on a fixed set of admissible logical symbols with an implicitly fixed semantics. This admits the use of sub-algorithms from symbolic computation. We are going to focus on quantifier elimination for the reals and its applications giving examples from geometry and verification. Beyond quantifier elimination we are going to discuss recent results on an incomplete decision procedure for the existential fragment of the reals, which has been successfully applied to the analysis of reaction systems in chemistry and in the life sciences. We conclude with an overview on further quantifier-eliminable theories that have been realized in our open-source computer logic software Redlog (www.redlog.eu).

Exploring a Homotopy Approach to the Science of Data: Huge Scenarios, Topological Scintigraphy and Flagellate Structures

Pedro Real
personales.us.es/real/

Abstract: Given a cloud of points (or dataset) embedded in some high dimensional space, Topological Data Analysis focuses on recovering topological information of an unknow lower dimensional space within which the previous dataset is sampled. At present, this information is obtained mainly using algorithms for computing persistent homology. In this talk, we introduce some basic notions and algorithms for providing a more advanced topological analysis of the datasets, based on homotopy concepts and higher order (co)homological statistics. This theory generating asymmetric topological dynamics in a "huge" or "classifying" data scenario is presented here using the relevant and informative analogy of "breathing topological life to a digital image". The promising conclusions regarding not only the power of topological discrimination of this technique but also its potential feasibility of a parallel processing allow to be optimistic about opening a door to a new area of Data Analysis: Homotopy-based Data Analysis and Recognition.

Sponsor Talks

What's New in Mathematica?

Simone Szurmant
Simone.Szurmant@additive-net.de

What's New in Maple 2016?

Jürgen Gerhard
GerhardJuergen@web.de

Abstract: We will present some of the new features in Maple 2016, in the areas of thermophysical computations, structured data manipulation, physics, series and limit computations, symbolic integration and summation, differential equations, statistics, graph theory, and others, and discuss some applications.

S1
Computer Algebra for Modeling in Science and Engineering

Application of Computer Algebra System and the Mean-Value Theory for Evaluating Electrostatic Potential and its Associated Field for Nontrivial Configurations

Haiduke Sarafian

The Pennsylvania State University, University College, York, PA, 17403

Evaluation of electrostatic potential at an arbitrary point within a two dimensional region free of electric charge containing geometrically dispersed nontrivial configurations electrified to constant potentials applying the standard classic approach, i.e. Laplace equation is challenging. The challenge stems from the fact that the solution of the Laplace equation needs to be adjusted to the boundary conditions imposed by the configurations. Numeric solution of the latter is challenging as it lacks generalities. An entirely different numeric solution method is based on the application of The Mean-Value Theory. The latter is a pure numeric approach; although the output of its iterated refined version is successful, it is cumbersome. In this investigation utilizing the powerful features of Computer Algebra Systems (CAS), specifically *Mathematica* by a way of example we show an innovative approach. Our approach is based on a combination of numeric aspect of The Mean-Value Theory on one hand and *Mathematica* features on the other hand. This semi numeric-symbolic approach not only provides the desired output, but it also generates information beyond the scope of the standard classic method. By way of example we present the intricacies of our approach, showing 1) how the potential is evaluated and 2) how corollary information not addressed in classic cases such as electric field is calculated as well. Our method is applied to a two-dimensional case; its three dimensional version may easily be applied to cases of interest.

1 Motivations and Goals

In two dimensional electrostatic it is a classic practice to map the potential that arises from a single common geometric object such as a line, a square, a circle and etc that is electrified to a potential. Stepping away from these cases one encounters multiple-body geometric configurations, each charged to a certain potential. Addressing the latter not only theoretically is interesting but is valued for practical applications. Analytic solutions of these scenarios mathematically are challenging and because each scenario embodies a specific configuration, solutions lack the generalities. The mathematical challenges stem from the fact that the potential,

ϕ that is subject to Laplace equation, $\nabla^2\phi = 0$ ought to be in compliance with the boundary conditions imposed by the geometry of the configuration. As such, in most cases one relies on the numeric solution of the Laplace equation [1],[2],[3]. An entirely alternative approach to addressing the same issue is a pure numeric method of another sort. This method by-passes the Laplace equation in its entirety; it is called The Mean-Value Theory, see for instance its applications [4]. Generally speaking one drops a virtual fishnet on the given configuration dividing the region of interest in grids. To begin with one assigns a wisely chosen guesstimated numeric potential to each node of the grid. Then one replaces the initial nodal potentials with the average of the potentials of the closest nodes. Repetition of the procedure stabilizes the potentials. The accuracy of the output is controlled by 1) recursive repetitions and 2) the fishnet mesh size; the smaller the mesh the better the output. This method appears to require either cumbersome manual or programming efforts.

Being aware of the latter issues, we present an effective, a short-cut approach curing both aforementioned challenges. The core of the solution is based on utilizing a Computer Algebra System (CAS) specifically *Mathematica* [5],[6]. To demonstrate the approach we craft our investigation that is composed of three sections. In addition to Motivations and Goals, in Section 2 by a way of example we present the detailed analysis. This section also includes the results and associated graphic output. Having this information on hand we further the analysis by evaluating the electric field. This is a fresh idea, literature lacks this information. We close our work with a few remarks.

2 Physics of the problem and its solution

Consider a set of two two-dimensional kinked metallic structure shown in Fig 1. The segments symmetrically are separated with a gap, and horizontally are extended to infinity. Assume the bottom and the top pieces are electrified to constant potentials e.g., $\phi = 0$ and $\phi = 3.0V$, respectively. The given structure resembles the profile of an unusual parallel-plate capacitor; this structure is suggested in [7]. It is one of the objectives of this investigation to determine the electrostatic potential at any point within the plates.

According to what is outlined in Sect. 1, in order to evaluate the potential we drop a fishnet with a coarse mesh size on the region of interest. This is shown in Fig 1.

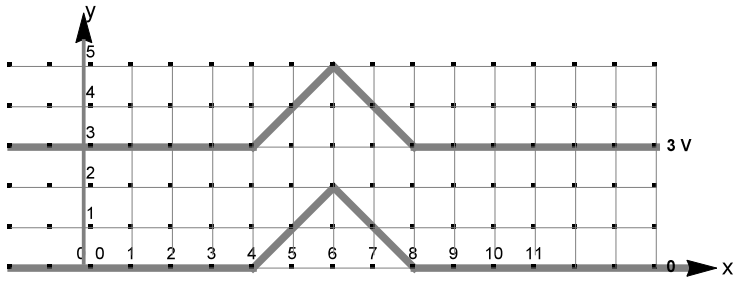


Figure 1. Display of the kinked structure with its accompanied fishnet grid.

The origin of the coordinate system conveniently is set as shown. The fishnet is composed of a 5*x11* grid. The node at the top left is p[1,1] and the one at the bottom right is p[6,11]. The matrix below is the intuitive nodal start-up potential assignment of the entire grid; potential of the exterior nodes are designated by x.

$$\begin{pmatrix} x & x & x & x & x & 3. & x & x & x & x & x \\ x & x & x & x & 3. & 2. & 3. & x & x & x & x \\ 3. & 3. & 3. & 3. & 2. & 1. & 2. & 3. & 3. & 3. & 3. \\ 2. & 2. & 2. & 2. & 1. & 0. & 1. & 2. & 2. & 2. & 2. \\ 1. & 1. & 1. & 1. & 0. & x & 0. & 1. & 1. & 1. & 1. \\ 0. & 0. & 0. & 0. & x & x & x & 0. & 0. & 0. & 0. \end{pmatrix}$$

Utilizing this input we apply the nearest averaging values; for the scenario at hand only four values would contribute. In other words one fourth of the sum of the four closest adjacent nodal potentials of the start up values replaces the initial chosen node's potential. Repetition of the procedure stabilizes the potentials. The presentation version displays two matrices after one and four repetitions, respectively.

As shown, the difference between the chosen nodal potentials for the scenario at hand just after only four recursions are negligibly small; i.e. potentials are stabilized. Customarily, for two distinct reasons 1) to achieve a higher numeric accuracy and 2) more importantly, for determining the potential at any point one is to refine the mesh size. This is straightforward; however, it is cumbersome. Instead we devised a fresh, innovative approach. We utilize *Mathematica* numeric interpolation. This operation utilizes the stabilized nodal potentials and in one step produces a refined output as if an extremely fine mesh is used. What follows is the numeric and accompanied graphic output of the interpolated procedure.

y	V(Volt)
2.	0.
2.2	0.426844
2.4	0.813969
2.6	1.16306
2.8	1.47581
3.	1.75391
3.2	1.99903
3.4	2.21288
3.6	2.39713
3.8	2.55347
4.	2.68359
4.2	2.78919
4.4	2.87194
4.6	2.93353
4.8	2.97566
5.	3.

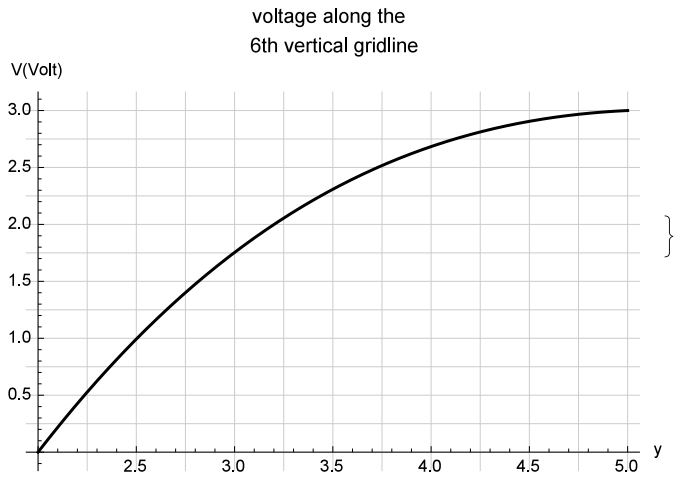


Figure 2. The first column of the table is the ordinates of the nodes. The second column is the corresponding potentials. The graph is the display of the adjacent table.

As shown the first column of the table includes not only the discrete integer y-values of the nodes but ordinates of the points between the nodes. Consequently, as explained in the text utilizing interpolation the second column embodies the corresponding potentials. The adjacent graph is the display of the Table. Accordingly, the interpolated plot gives the potential of any arbitrary y-valued ordinate. For the sake of clarification the output of this procedure is detailed for the 6th vertical grid-line. One may follow the same approach tabulating and plotting curves for any of the vertical grid-lines. Next we extend the procedure for horizontal grid lines with ordinates of 1,2 and 3. These are shown in Fig 3. Each set of curves is composed of a pair of lines. The dashed lines represents the point-to-point connected curves; the smooth solid lines are the interpolated curves.

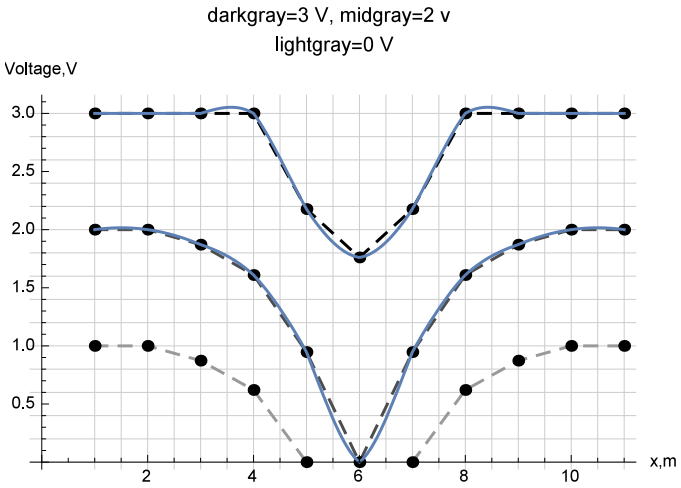


Figure 3. Coordinate of the x-axis is the same as the coordinate of the grid-lines in Fig 1. Dots are the potentials corresponding to the last matrix in the text. The dashed lines are the point-to-point connected curves. The smooth solid curves are the interpolated potentials.

With this information at hand utilizing, $\vec{E} = -\vec{\nabla}\phi$ surprisingly we are able to calculate the associated electric fields. This procedure embodies two valued points: 1) as shown the interpolated data is a continuous function making the gradient operable. Otherwise we would have to replace the gradient with a difference equation i.e., $\frac{\Delta\phi}{\Delta\xi}$where ξ is the distance between the potential contours. This would have given less accurate fields. 2) As shown in Fig 3 potential is a two dimensional function, $\phi(x,y)$ so that its associated field is a two dimensional vector, $\{E_x, E_y\}$. For a sake of completeness two such continuous fields associated with two grid-lines are tabulated and graphed. Presentation version displays the tables and their associated figures.

By tabulating and plotting these fields we illustrate that with a coarse mesh shown in Fig 1 we are able to evaluate the fields as if the mesh was refined and optimized.

3 Conclusions

Obtaining analytic solution even for two dimensional semi complicated geometrically dispersed electrified objects is challenging. Laplace equation is the master equation that needs to be adjusted to the relevant boundaries; this makes the solution peculiar to a specific scenario, as such it lacks generalities. An alternative

solution other than numeric solution of Laplace equation is the Mean-Value Theory. This requires refined cumbersome programming. In this investigation we show utilizing a Computer Algebra System (CAS), specifically *Mathematica* a less cumbersome, satisfactory shortcut solution can be obtained. By way of example we present the specifics of our approach. For the sake of completeness we utilize the numeric output of the analysis and semi-analytically computed axillary quantities such as the fields. The presented approach conveniently may be applied to configurations of interest and readily may be extended to 3D configurations.

References

[1] Gilberto Urroz, Numerical Solution of Laplace Equation, ocw.usu.edu/LaplaceDirichletTemperature.pdf

[2] B. Hansen, Numerical Solution of Laplace's Equation, Syracuse University, New York 13244, 1992.

[3] Nunerical Solutions to Laplace's Equation, PHY220C (Electromagnetic Fields), newton.ex.ac.uk/teaching/CDHW/EM/CW960313-2.pdf

[4] B.A. Kemp, et al, Application of the electrostatic mean-value theorem to electrostatic sensor electrodes, Journal of Electrostatic - 65 (2007) 69-74, Elsevier.

[5] Mathematica^{TM} is symbolic computation software, V10.3, Wolfram Research Inc., 2015.

[6] Stephen Wolfram, "Mathematica book", 3rd ed., Cambridge University Press, 1996.

[7] Hans Ohanian, "Physics", 2nd ed. Expanded, W.W. Norton & Company, Inc., 500Fifth Ave., New York, 1989.

Experimental and Finite Elements Stress Analysis of a Double Edge Notched Specimen

A. Bilek[1], M. Beldi[1], T. Cherfi[1], S. Djebali[1], S. Larbi[1],

[1] *LMSE Laboratory, Mechanical Engineering Department, UMMTO University, Tizi-Ouzou, Algeria, alibilek@ummto.dz*

Photoelasticity and finite elements analysis are used to determine the stress field developed in a birefringent double edge notched specimen loaded in tension. Experimental isochromatic fringes and isoclinics fringes are obtained on a regular polariscope by using circularly polarized light and plane polarized light. Simulated isochromatic fringes and isoclinic fringes are obtained particularly in the neighborhood of the notches. The shear stress along the weakened cross section in the neighborhood of the notches are determined numerically and experimentally with the help of the isochromatic fringe pattern. Details of the procedure are fully given in the paper. Relatively good agreements are obtained between the experimental and the simulated results.
Keywords: Isochromatic, isoclinic, stress, birefringent, notch

1 Introduction

In stress analysis experimental procedures can sometimes be time consuming and theoretical studies can also be in some cases very complex. Numerical solutions can therefore be very helpful. Various authors (see Refs. [1, 8]) have used experimental techniques as well as finite elements analysis to solve these kinds of problems. In this study, a stress field is applied to a double edge notched specimen (see Fig. 1); the load is applied in a loading frame equipped with a dynamometer that measures the applied load. The stress field is then determined experimentally on the analyzer of a regular polariscope by using both plane polarized light and circularly polarized light. The isochromatic fringe pattern is used to determine stress values, particularly in the neighborhood of the notches. A finite element analysis is used to simulate the isochromatic fringe pattern and the isoclinic fringe pattern for comparison purposes. We consider that the material of the model behaves as a purely isotropic material. To achieve better approximation, the mesh is refined in the neighborhood of the contact zone.

2 Theory and experimental procedure

Fig.1 shows the photoelasticity method which is based on the birefringent phenomenon. In some transparent isotropic materials an incident light beam splits in two independent light beams which travel through the model thickness at different velocities $v1$ and $v2$. The corresponding refractive indexes $n1$ and $n2$ depend on the principal stresses developed in the stressed model. In the light intensity obtained with plane polarized light on the analyzer of a polariscope (see Eq. (1)), the terms $\sin^2 2\alpha$ and $\sin^2 \varphi/2$ give respectively the isoclinic fringes and the isochromatic fringes [9].

$$I = a^2 \sin^2 2\alpha \sin^2 \varphi/2 \tag{1}$$

The isochromatics (loci of points of equal maximum shear stress) are used to determine the principal stresses difference in the whole model particularly in the neighborhood of the notches (see Eq. (2)).

$$\sigma_1 - \sigma_2 = \frac{N(\lambda/C)}{e} \tag{2}$$

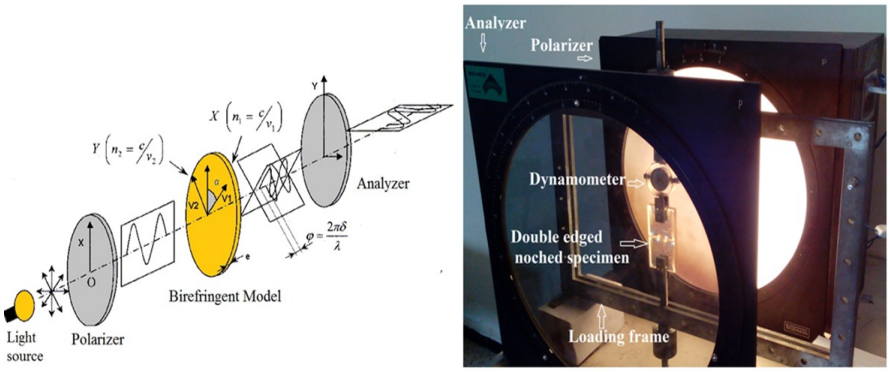


Figure 1: Light propagation through a photoelastic model and experimental setup.

3 Experimental results

The isochromatic fringe pattern (see Fig. 2) is obtained on a white field circular polariscope, two quarter wave plates are added in the light path in order to eliminate the isoclinic fringes that can hide the isochromatic fringes. The isochromatic fringe pattern is then recorded for further analysis. The fringe orders are easily

determined from the isochromatic fringe pattern (see Fig. 2), the first order being $N = 0.5$ since we use a white field. In the neighborhood of the notches we observe higher fringe orders as one might expect. The fringe orders in the neighboorhood of the contact zone are determined easily and accurately by zooming in the neighboorhood of the notch (see Fig. 2 right) in order to obtain the principal stresses difference for comparison purposes with the finite element solution. The order reaches $N = 10.5$ near the tip of the notch. The following values given here after are used to implemente the experimental solution as well as the numerical one: Young's modulus ($E = 2437N/mm^2$), Poison's ratio ($\mu = 0.37$), applied load ($F = 850N$) and fringe value ($f = \lambda/C = 11N/mm/fringe$).

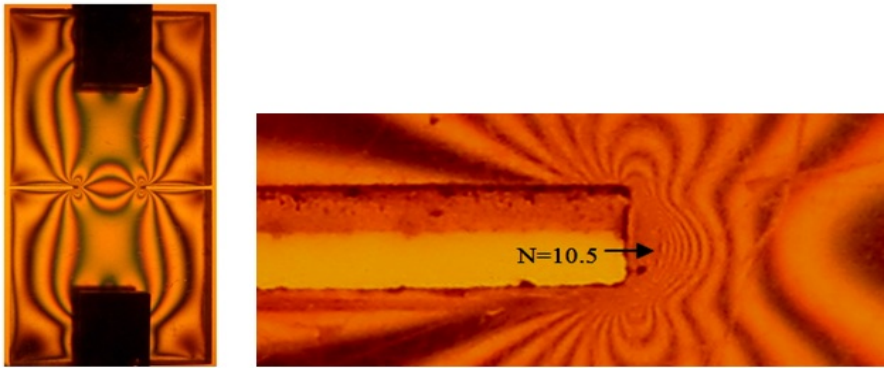


Figure 2: Experimental isochromatic fringes (left), Close-up of the notch (right).

4 Finite elements analysis

Since we are using two dimensional photoelasticity, we understand that we are dealing with plan stress problems, stresses do not vary along the thickness of the model. Therefore, in the finite element solution we simply consider that the stress is constant along the thickness. The meshing of the model is refined in the in the neighborhood of the notches to obtain more accurate results. The details of the procedure are shown here after.

4.1 Isoclinic reconstruction

The values of the isoclinic parameter are calculated with the following relation (see eq. (3)) that can be readily obtained from Mohr's circle of stresses.

$$\alpha = \arctan(2\tau_{xy}/(\sigma_x - \sigma_y)) \tag{3}$$

The isoclinic fringes ($\sin^2 2\alpha$) can therefore be calculated for different polarizer and analyzer settings. In the finite elements solution a color scale is used to represent the different values of the isoclinic term. On the reconstructed isoclinic fringe pattern, the blue color corresponds to a dark isoclinic fringe obtained experimentally on the analyzer of a plane polariscope.

4.2 Isochromatic reconstruction

Isochromatic fringes are calculated with the term $\sin^2 \varphi/2$. Using Mohr's stress relations and (Eq.2), one can easily obtain the values of the isochromatic parameter φ, the isochromatic parameter (see Eq. (4)).

$$\varphi = \frac{2\pi e}{(\lambda/C)} \sqrt{(\sigma_x - \sigma_y)^2 + 4\tau_{xy}^2} \tag{4}$$

The program calculates the isochromatic fringe pattern on the whole model. In the color scale used by the software, the blue color corresponds to a dark isochromatic fringe.

5 Comparison between experimental and simulated results

5.1 Experimental and simulated isochromatic fringes

The experimental and the simulated isochromatic fringe patterns (see Fig.3) are relatively similar; the blue simulated isochromatic fringes correspond to the dark experimental isochromatic fringes. We see clearly a concentration of isochromatic fringes in the neighbourhood of the notches. In the finite element solution we see also stress concentrations in the neighbourhood of the holes but these are not taken into account in this study as the experimental loading frame hides this zone. We are therefore mainly interested in the stress fields developed in the neighbourhood of the notches.

We can see relatively good agreements between experimental values and numerical ones (see Fig. 3). Stresses are higher in the vicinity of the notches, and then decrease to a lower constant value.

5.2 Experimental and simulated isoclinic fringes

One should know that experimentally it is not possible to obtain the isoclinics alone. We have therefore, on the recorded experimental photoelastic fringes, both the isochromatics which appear in color when we use polychromatic light and the

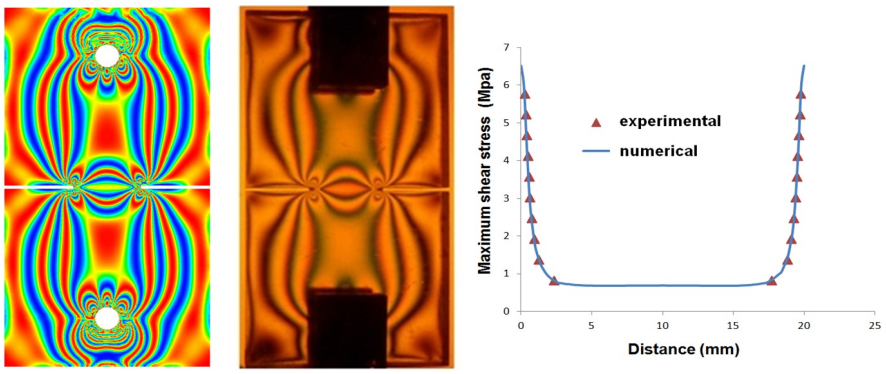


Figure 3: Experimental and simulated isochromatic fringes and shear stress in the neighbourhood of the notches.

isoclinics. We show the isoclinics for four positions of the polarizer and the analyzer axis (see Fig. 4). We can see relatively good agreements between the simulated and the experimental isoclinics, the blue color corresponds to a dark isoclinic fringe. The isoclinics can further be used to determine the stress trajectories called also isostatics.

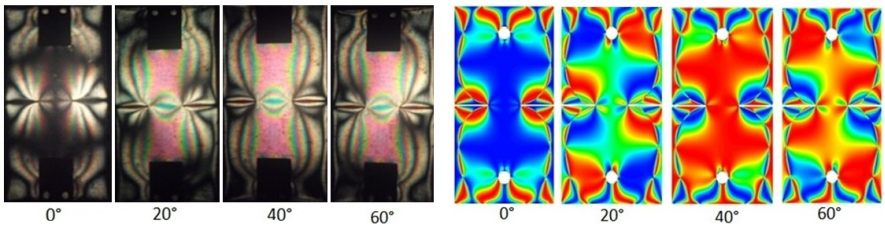


Figure 4: Experimental and simulated isoclinic fringes.

6 Conclusion

We have analysed a stress field developed in a birefringent double edge notched specimen by using photoelasticity and finite element analysis. The purpose is to analyse the stress field, particularly in the neighbourhood of the notches. We showed that photoelastic fringes and stresses can be simulated easily and accurately. Since the fringe order at the notch tip is difficult to determine experimentally, stress at the notch tip is determined more accurately with the finite element analysis and this is of great importance in the design of mechanical components.

References

[1] A. Germaneau, F. Peyruseigt, S. Mistou, P. Doumalin and J.C. Dupré, *Experimental study of stress repartition in aeronautical spherical plain bearing by 3D photoelasticity : validation of a numerical model, 5th BSSM* , International Conference on Advances in Experimental Mechanics, University of Manchester, UK Sept. 2007.

[2] Choon Tae Lee, Myung Soo Kim and Tae Hyun Baek, *Stress concentration factor measurement of tensile plate with circular and elliptical hole by digital hybrid photoelastic experiment*, Advanced Science and Technology Letters, **64** Mechanical Engineering 214, pp. 35-38 (2014).

[3] Abodol Rasoul Sohouli, Ali Maozemi Goudarzi, Reza Akbari Alashti, *Finite Element Analysis of Elastic-Plastic Contact Mechanic Considering the Effect of Contact Geometry and Material Propertie*, Journal of Surface Engineered Materials and Advanced Technology , 1, pp. 125-129 (2011).

[4] A. Bilek, J.C. Dupré , A. Ouibrahim, F. Bremand, *3D Photoelasticity and numerical analysis of a cylinder/half-space contact problem* , Computer Methods and Experimental Measurements for Surface Effects and Contact Mechanics VII, WIT Press Southampton, Boston, pp. 173-182 (2005).

[5] Budimir Mijovicand Mustapha Dzoclo, *Numerical contact of a Hertz contact between two elastic solids*, Engineering Modeling 13 , pp. 111-117 (2000).

[6] T. L. Nguyen, A. Fatu, D. Souchet,*contact entre le coussinet et le logement dans un palier lisse*,21ème Congrès Français de Mécanique, bordeaux (2013).

[7] invydas Ragulskis, Violeta Kravcenkiene, Liutauras Ragulskis, *Image processing algorithm for plotting isoclinics in photoelastic analysis*, ISSN 1392-124X Informacin's Technologijos Irvaldymas , Nr.1(30) (2013).

[8] Ramesh, K., Kasimayan, T., Neethi, Simon, B.*Digital photoelasticity - A comprehensive review*. *The Journal of Strain Analysis for Engineering Design*, **46**, 4: pp. 245-266 (2011).

[9] J. W Dally and F. W. Riley, *Experimental stress analysis*, McGraw-Hill, Inc, (1991).

Modelling and Simulation of Solid Particle Sidementation in an Incompressible Newtonian Fluid.

S. Zouaoui[1], H. Djebouri[1], A. Bilek[1], K. Mohammedi[2]

[1] *LMSE Laboratory, Mechanical Engineering Department, UMMTO University, Tizi-Ouzou, Algeria, alibilek@ummto.dz; zouaouisalah@ummto.dz*
[2] *LEMI Laboratory MESO, M'Hamed Bougara University of Boumerdes 35000, Algeria, mohammedi.meso.lemi@gmail.com*

1 Introduction

The understanding of the physical phenomena that govern fluid / particle flows is continuously improving, particularly in the last decade. Transport phenomena and solid particles deposit in the context of hydraulic turbine engine systems is multi-disciplinary. For modeling and simulation of such flows, there are several methods which use dynamic meshing. These methods follows the movement of the objects in a Lagrangian way [1, 2, 3]. However, the remeshing steps can be expensive and very difficult, especially in the 3D case.

To overcome the constraints caused by the use of adaptive meshing and reduce the problems associated with linking steps, new methods with fixed meshing are used. These are also called methods of fictitious domain as they extend a problem defined on a mobile and complex area (the fluid domain) to a domain (fictional) larger but fixed. **R. Glowinski et al** (see [4, 5, 6, 7, 8, 9]) are the investigators of fictitious domain methods. If the fixed field is sufficiently simple, this kind of method allows the use of Cartesian meshes, which allows the use of fast solvers.

Although the Navier-Stokes equations describing the behavior of a fluid still admit no evidence of existence of a general solution, they are still widely used to describe Newtonian fluid flows. In the case of the presence of particles in the fluid, the processing of the interaction between the fluid phase and the solid phase adds complexity to the studied problem.

In this paper we present a method of simulating the movement of one or more convex rigid body in a Newtonian incompressible fluid. We used a penalty method which is based on a reformulation of the stress tensor which allows the canceling of the deformation rate in the volume occupied by the particle. This method consists on constraining the movement of the fluid to be the same as the movement of

a particle by increasing locally the viscosity of the fluid [10, 11, 12]. This method has been used by many authors, initially to consider the Dirichlet condition at the edge of the field, and then to deal with the presence of an obstacle within a flow. It has been expanded recently to deal with the stress of rigid motion for a particle in a fluid for a finite differences approach then for finite elements [13, 14].

The objective of this work is to develop a code from FreeFem ++ that simulates Stokes or Navier-Stokes flows (with low Reynolds number) in the presence of solid particles. A test case on the sedimentation of a particle is presented.

2 Mathematical formulation of the problem

We consider a connected, bounded and regular domain $\Omega \subset \mathbb{R}^2$ (see Fig.1) and we denote by $(B_i)_{i=1,\cdots,N}$ the rigid particles, strongly included in Ω. B denotes the whole rigid domain: $B = \cup_i B_i$. The domain $\Omega \setminus \overline{B}$ is filled with Newtonian fluid governed by the Navier-Stokes equations. We note μ the viscosity of the fluid, p the presure and $\mathrm{f_f}$ the external forces exerted on it. Since we consider a Newtonian fluid, the stress tensor $\underline{\underline{\sigma}}$ is given by the following relation (see Eq. (1)):

$$\underline{\underline{\sigma}} = 2\mu\mathbb{D}(\mathbf{u}) - p\mathbb{I}, \quad \text{where} \quad \mathbb{D}(\mathbf{u}) = \frac{\nabla(\mathbf{u}) + (\nabla(\mathbf{u}))^T}{2} \tag{1}$$

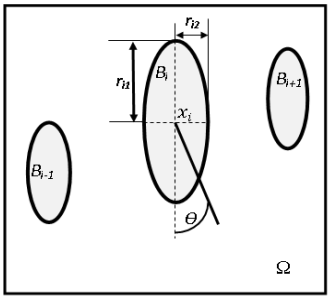


Figure 1: Partcicles B_i in a Newtonian fluid.

We consider homogeneous Dirichlet conditions on $\partial\Omega$. The presence of viscosity imposes a no-slip condition on the boundary ∂B of the rigid domain.
At the initial time the particles with density ρ_i are distributed randomly over the fluid. The position of the center of the ith particle is denoted by x_i, by v_i and ω_i its translational and angular velocities. We denote by m_i and J_i the mass and the kinematic momentum about its center of mass:

$$m_i = \int_{B_i} \rho_i, \quad J_i = \int_{B_i} \rho_i \|x - x_i\|^2 \tag{2}$$

We have to find the velocity $\mathrm{u}(u_1, u_2)$ and the pressure field p defined in $\Omega \setminus \overline{B}$, as well as the velocities of the particles$\mathbf{V} := (\mathrm{v}_{\mathrm{i}=1,\ldots,\mathrm{N}}) \in \mathbb{R}^{2N}$ and $\omega := (\omega_{\mathrm{i}=1,\ldots,\mathrm{N}}) \in \mathbb{R}^N$ such that (see Eq. (3)):

$$\begin{cases} \rho_{\mathrm{f}}(\frac{\partial \mathbf{u}}{\partial t} + \mathbf{u}.\nabla \mathbf{u}) - \mathrm{div}(\underline{\sigma}) = \mathbf{f}_{\mathrm{f}} & \text{dans } \Omega \setminus \overline{B}, \\ \mathrm{div}(\mathbf{u}) = 0 & \text{in } \Omega \setminus \overline{B}, \\ \mathbf{u} = 0 & \text{on } \partial\Omega, \\ \mathbf{u} = \mathbf{v}_i + \omega_i (x - x_i)^{\perp} \text{ on } \partial B, \ \forall i \in \{1, \ldots, N\} \end{cases} \tag{3}$$

where ρ_{f} denotes the density of the fluid and $\mathbf{f}_{\mathrm{f}} = \rho_{\mathrm{f}} g e_y$ is the external force exerted on the fluid (gravity forces). The fluid exerts hydrodynamic forces on the particles. Newton's second law for these particles is written then as follows (see Eq. (4)):

$$\begin{cases} m_i \frac{dV_i}{dt} = \int_{B_i} \mathrm{f_i} - \int_{\partial B_i} \underline{\sigma} n, \\ \\ J_i \frac{d\omega_i}{dt} = \int_{B_i} (x - x_i)^{\perp}.\mathrm{f_i} - \int_{\partial B_i} (x - x_i)^{\perp}.\underline{\sigma} n, \end{cases} \tag{4}$$

Where, $\mathrm{f_i}$ denotes the external non-hydrodynamical forces exerted on the sphere, such as gravity : $\mathrm{f_i} = -\rho_i g e_y$.

3 Variational formulation and Penalisation method

The variational formulation obtained on the whole fluid/particle domain Ω is given here after (see Eq. (5)):

$$\begin{cases} \textit{Find } (\mathbf{u}, p) \in \mathbf{K}_B \times \mathbf{L}^2_0(\Omega) \textit{ suchthat} \\ \\ \int_\Omega \tilde{\rho} \frac{D\mathbf{u}}{Dt} \mathbf{v} + 2\mu \int_\Omega \mathbb{D}(\mathbf{u}) : \mathbb{D}(\mathbf{v}) - \int_\Omega p \mathrm{div}(\mathbf{v}) = \int_\Omega \tilde{\mathrm{f}}.\mathbf{v}, \ \forall \mathbf{v} \in \mathbf{K}_B \\ \\ \int_\Omega q \mathrm{div}(\mathbf{u}) = 0, \ \forall q \in \mathbf{L}^2_0, \end{cases} \tag{5}$$

with $\tilde{\rho} := \rho_f \mathbf{1}_{\Omega \setminus \overline{B}} + \sum_{i=1}^N \rho_f \mathbf{1}_{B_i}$, $\quad \tilde{\mathrm{f}} := \mathrm{f}_f \mathbf{1}_{\Omega \setminus \overline{B}} + \sum_{i=1}^N \mathrm{f}_i \mathbf{1}_{B_i}$ *and* $\mathbf{K}_B = \{\mathbf{u} \in H^1_0(\Omega) \mathbb{D}(\mathbf{u}) = 0 \, in B\}$.
Using a penalty method, we will rather consider the following problem:

$$\begin{cases} Find\ (\mathbf{u},p) \in \mathbf{H}_0^1(\Omega)\times \mathbf{L}^2(\Omega)\ such that \\ \int_\Omega \tilde{\rho}\frac{D\mathbf{u}}{Dt}\mathbf{v} + 2\mu \int_\Omega \mathbb{D}(\mathbf{u}):\mathbb{D}(\mathbf{v}) + \frac{2}{\varepsilon}\int_B \mathbb{D}(\mathbf{u}):\mathbb{D}(\mathbf{v}) \\ \qquad\qquad - \int_\Omega p\,\mathrm{div}(\mathbf{v}) = \int_\Omega \tilde{\mathrm{f}}.\mathbf{v},\ \forall \mathbf{v}\in \mathbf{H}_0^1(\Omega), \\ \qquad\qquad \int_\Omega q\,\mathrm{div}(\mathbf{u}) = 0,\ \forall q \in \mathbf{L}^2(\Omega), \end{cases} \tag{6}$$

The variational formulation (see Eq. (6)) shows that the physics behind this method is to consider the rigid domain as a fluid with infinite viscosity.
The time discretization is performed by using the method of characteristics [15].

4 Results

In Fig. 2, we show the results of the sedimentation of elliptic particle in a closed box filled with a Navier-Stokes fluid at different time steps.

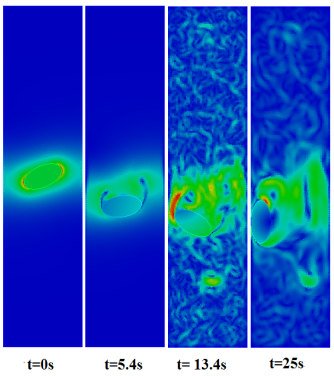


Figure 2: Sedimentation of particule -configurations at different time steps-

5 Conclusion

In this paper, we have proposed a strategy for the numerical modeling of the motion of a convex rigid particle in a Newtonian fluid. The rigid motion is imposed by penalizing the strain tensor, the time discretization is performed by using the method of characteristics.

The code was written in FreeFem++ version 3.26 and at each time step the generalized Navier-Stokes problem is solved by using standard finite elements.

References

[1] Hu, Howard H and Patankar, Neelesh A and Zhu, MY *Direct numerical simulations of fluid–solid systems using the arbitrary Lagrangian–Eulerian technique*, Journal of Computational Physics **169**, 2, pp. 427-462 (2001).

[2] A. Lefebvre and B. Maury *Apparent viscosity of a mixture of a Newtonian fluid and interacting particles*, Comptes rendus mécanique **333**, 12, pp. 923–933 (2005).

[3] B. Maury *Direct simulations of 2D fluid-particle flows in biperiodic domains*, Journal of computational physics **156**, 2, pp. 325-351 (1999).

[4] C.Atamian, and P. Joly *Une analyse de la méthode des domaines fictifs pour le problème de Helmholtz extérieur*, RAIRO-Modélisation mathématique et analyse numérique **27**, 3, pp. 1251-288 (1993).

[5] R. Glowinski, Pan, Tsorng-Whay, Todd I Hesla, and Joseph Daniel D and J. Periaux. *A fictitious domain method with distributed Lagrange multipliers for the numerical simulation of particulate flow*, Contemporary mathematics **218**, pp. 121–137 (1998).

[6] R. Glowinski and Y. Kuznetsov. *On the solution of the Dirichlet problem for linear elliptic operators by a distributed Lagrande multiplier method*, Comptes Rendus de l'Académie des Sciences-Series I-Mathematics **327**, (2002).

[7] V. Girault, R.Glowinski and TW.Pan. *A fictitious-domain method with distributed multiplier for the Stokes problem*, Applied nonlinear analysis **327**, 7, pp. 159-174 (2002).

[8] V. Girault, R.Glowinski and TW.Pan. *A distributed Lagrange multiplier/fictitious domain method for flows around moving rigid bodies: application to particulate flow*, International Journal for Numerical Methods in Fluids **30**, 8, pp. 1043-1066 (1999).

[9] R. Glowinski, TW. Pan,T I. Hesla, DD. Joseph and J.Periaux. *A fictitious domain approach to the direct numerical simulation of incompressible viscous flow past moving rigid bodies: application to particulate flow*, Journal of Computational Physics **169**, 2, pp.363-426 (2001).

[10] J. Caltagirone and S. Vincent. *Tensorial penalisation method for solving Navier-Stokes equations*, Comptes Rendus de l'Academie des Sciences Series IIB Mechanics **329**, 8, pp.607-613 (2001).

[11] S.Vincent, JSB. De Motta, A. Sarthou, JL. Estivalezes, O. Simonin and E. Climent. *A Lagrangian VOF tensorial penalty method for the DNS of resolved particle-laden flows*, Journal of Computational Physics **256**, pp.582-614 (2014).

[12] S Vincent, TN Randrianarivelo, G Pianet and JP. Caltagirone. *Local penalty methods for flows interacting with moving solids at high Reynolds numbers*, Computers & fluids **36**, 5, pp.902-913 (2007).

[13] J. Janela, A. Lefebvre and B. Maury. *A penalty method for the simulation of fluid-rigid body interaction*, ESAIM: Proceedings **14**, pp.115–123 (2005).

[14] A.Lefebvre. *Fluid-particle simulations with FreeFem++*, ESAIM: Proceedings **18**, pp.120-132 (2007).

[15] O. Pironneau, J.Liou and T.Tezduyar, *Characteristic-galerkin and galerkin/least-squares space-time formulations for the advection-diffusion equation with time-dependent domains*, Computer Methods in Applied Mechanics and Engineering **100**, pp.117-141 (1994).

Interfacing KetCindy and CASs, and its Applications to Scientific Problems Modeling

Setsuo Takato[1], José A. Vallejo[2], Masataka Kaneko[3]

[1] *Toho University, Japan, takato@phar.toho-u.ac.jp*
[2] *Universidad Autónoma de San Luis Potosí, México, jvallejo@fc.uaslp.mx*
[3] *Toho University, Japan, masataka.kaneko@phar.toho-u.ac.jp*

1 Introduction

Nowadays the majority of college math instructors use LaTeX when preparing materials for their classes. LaTeX is a powerful editor specifically designed for writing scientific and mathematical formulas. In this regard, the scope of its capabilities ranges from the simplest to the most complex. However, it falls somewhat short when it comes to dealing with graphics. Making graphics with LaTeX can be a challenging and cumbersome task, requiring additional coding skills that can divert the attention from the main goal, which is teaching the subject matter.

What most LaTeX users do is to create their graphics with the aid of a separate program and then import them in the working LaTeX document. Of course, more advanced users can resort to TiKZ, which is a TeX package with its own commands and syntax, but this is difficult for the beginner or the occasional user, due to the steep learning curve. To overcome this issue the authors developed a package called KeTpic[1], using a CAS to generate the LaTeX code for graphics. Here is a quick example of how it works: A CAS (say, Scilab [2]) user would download the folder `ketpicsciL5` and the file `ketpic.sty` both from [1]. For definiteness, suppose that, in a Linux box, they are downloaded to the directory `/home/username/ketpic`. Then, in a Scilab session the user would write the following sequence of commands:

```
cd("/home/username/ketpic");
Ketlib=lib("ketpicsciL5");
Ketint();
gr1=Plotdata("x^2","x");
gr2=Lineplot([-1,1],[2,4]);
h1=Hatchdata("ii",list(gr1,"n"),list(gr2,"s"));
Openfile("fig1");
Drwline(gr1,gr2,h1);
Expr([2,4],"se","y=x+2",[2,5],"nw","y=x^2");
Closefile("1");
```

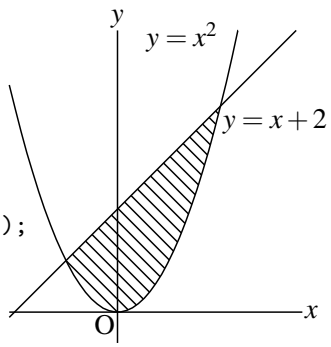


Figure 1

This creates a `fig1.tex` file in the directory `/home/username/ketpic`, containing the LaTeX code that generates Figure 1. To use it, the user must add `\usepackage{ketpic}` to the preamble of her document; then, the command line `\input{fig1.tex}` will do the job. The resulting .tex document should be compiled with XeLaTeX or LaTeX for better results.

2 Migration from KETpic to KETCindy

KETCindy[1] is an upgrade of KETpic which combines its features with those of the popular dynamic geometry software Cinderella. Cinderella works as a GUI for KETCindy: Graphics are shown in Cinderella via a KETCindy script while Scilab runs in the background. The interactive features of the latter allow editing the figures via the CindyScript editor. A brief procedural step of the process is shown in Figure 2.

1. Draw geometric objects on the Cinderella worksheet.
2. Write a script as in Section 1 to generate the LaTeX code for the figure.
3. Execute a batch process of Scilab, LaTeX compiler and a PDF viewer.

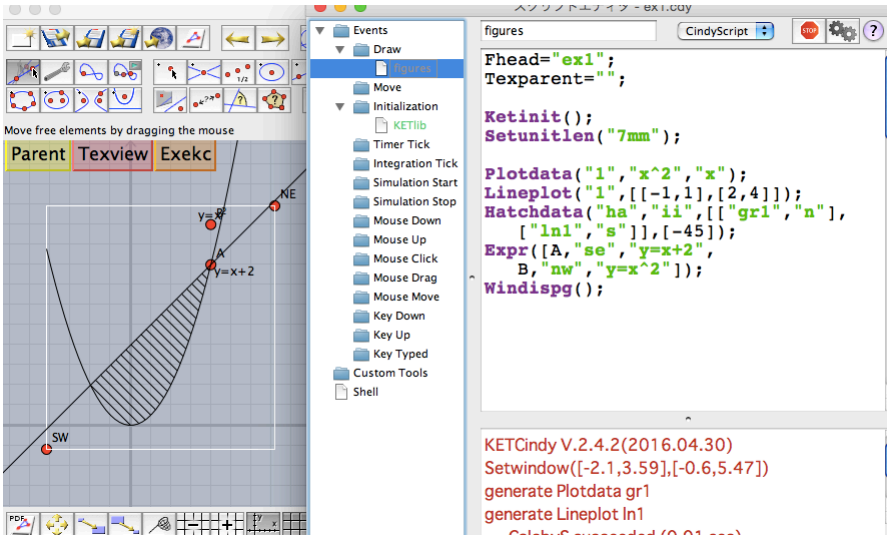


Figure 2

KETCindy's codes are short and compact, yet they generate high resolution images as good as KETpic's ones, suitable for inclusion in high quality documentation projects or research papers.

3 Interfacing with CASs

The most recent version of KETCindy includes capabilities of interfacing with Computer Algebra Systems others than Scilab. In this paper we illustrate the case of Maxima [4], but there exist versions for Fricas [5] and Risa/Asir [6]. The flow chart of these interfaces is shown in Figure 3.

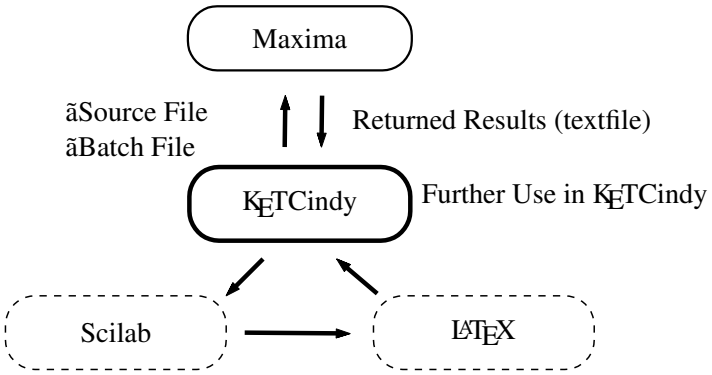


Figure 3

When interfacing with Maxima, the command `Mxfun` is all we need to complete the task. Other commands such as `calcbyM` and `Mxtex` may be used for multistep and code conversion to LaTeX, respectively. The output of the CAS is returned to KETCindy as a character string for further processing of the graphics. Used this way, KETCindy proves to be a powerful companion to CASs.

4 Examples

4.1 Fourier Series

The second author has developed a package for computing the Fourier series of piecewise defined functions in Maxima, called `fourier_sec`. Below we show the code needed to compute the Fourier expansion of degree 10 of a square wave.

```
cmdL=Concat(Mxbatch("fourier_sec"),[
  "hs(x):=if (x<0 and x>=-1) then 0 "
    +"elseif (0<=x and x<=1) then 1",[],
  "c:fourier_sec_coeff",["hs(x)","x"],
  "c[1]::c[2]::c[3]",[]
]);
CalcbyM("c",cmdL,[]);
```

```
c0=text(c_1); cn=text(c_2);
Mxtex("2",c_3);
sn=replace(c_3,"%pi","pi");
fs=c0;
forall(1..10,
  tmp1=assign("("+cn+")*cos(n*pi*x)","n",#);
  tmp2=assign("("+sn+")*sin(n*pi*x)","n",#);
  fs=fs+"+"+tmp1+"+"+tmp2;
);
Plotdata("2",fs,"x",["Num=400"]);
Expr([D,"e","s_n="+tx2,E,"e","n=10"]);
```

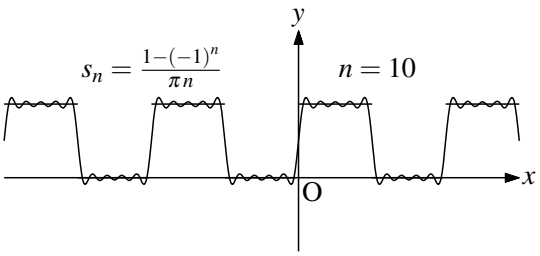


Figure 4

4.2 Generating 3D Models

One of the appealing features of KETCindy is its capability of displaying 3D graphics (through .obj files). These are to be viewed with programs such as Meshlab [7]. Once the basic 3D graphics has been coded, and prior sending the file to a 3D printer, using Maxima the surface can be fine-tuned by giving it the desired thickness (this is required by the 3D printing process), in addition to other features. The final code, along with its 3D printed version, is shown in Figure 5.

```
fd=["p","x=U*cos(V)","y=U*sin(V)","z=cos(V)^2-sin(V)^2",
  "U=[0,2]","V=[0,2*pi]","e"];
tmp=Mkobjnrm("1",fd);
cmdL=["assume",["U>0"],"a:trigsimp",[tmp],"a",[]];
CalcbyM("ans",cmdL);
Mxfun("1","solve",[den,"C"]);
cmdL=["assume",["U>0"],
  "a1:limit",[norm1,"V","0"],...];
CalcbyM("lim1",cmdL,[""]);
norm="if or(V==%p/2*[0,1,2,3,4]) then Out=[0,0,1];"
   +"else Out="+norm+";end";
cmd=Mkobjthickcmd("1",fd,norm,[0.05,"+n+s-e-w+"]);
Mkviewobj("ds",cmd),["m","v");
```

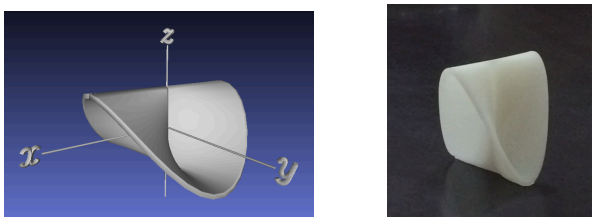


Figure 5

5 Conclusions

The goal of the paper is to show by way of examples how our package KETCindy can be used to generate high quality 2D and 3D graphics to be used within technical LaTeX documents. Also, a brief description of the interface between several CASs and LaTeX through KETCindy is presented.

Acknowledgments
This work was supported by JSPS KAKENHI Grant Numbers 25350370, 15K01037, 15K00944. The second author was partially supported by the Mexican Consejo Nacional de Ciencia y Tecnología, Project CB-2012 179115.

References

[1] KeTpic/KeTCindy, `http://ketpic.com/?lang=english`
[2] Scilab, `http://www.scilab.org`
[3] Cinderella, `http://www.cinderella.de`
[4] Maxima, `http://maxima.sourceforge.net`
[5] Fricas, `http://fricas.sourceforge.net`
[6] Risa/Asir, `http://www.math.kobe-u.ac.jp/Asir/asir.html`
[7] Meshlab, `http://meshlab.sourceforge.net`
[8] Kaneko M., Yamashita S., Kitahara K., Maeda Y., Nakamura Y., Kortenkamp U, Takato S., KETCindy— Collaboration of Cinderella and KETpic, Reports on CADGME 2014 Conference Working Group, The International Journal for Technology in Mathematics Education, 22(4), 179–185, 2015.
[9] Takato S., Hamaguchi N., Sarafian H., Generating Data of Mathematical Figures for 3D Printers with KETpicand Educational Impact of the Printed Models, ICMS 2014, LNCS, vol. 8592, pp. 629–634, Springer, Heidelberg, 2014.
[10] Kaneko M, Takato S., The effective use of LaTeX drawing in linear algebra, The Electronic Journal of Mathematics and Technology 5(2), pp. 1–20, 2011.

On the Visualization of Random Fibonacci-Padovan Sequences

T. Mylläri[1], A. Mylläri [1], A. Anckar [2], G. Högnäs [2]

[1] *St. George's University, Grenada, West Indies, amyllari@sgu.edu*
[2] *Åbo Akademi University, Turku/ Åbo, Finland*

Fibonacci numbers [1] are known for more than two thousand years, Padovan numbers are much younger, they were introduced only recently [2]. Viswanath in his classic paper [3] studied the growth rate of random Fibonacci sequences

$$f_n = f_{n-1} \pm f_{n-2}$$

and got the exponent 1.13198824... (named later Viswanath's constant). Gogin and Mylläri [4] studied the problem of the growth rate of random Fibonacci-Padovan sequences and showed that the average growth rate of such sequences in the case of equal probabilities, $\lim_{n\to\infty} \sqrt[n]{E(u_n)}$ is equal to the greatest positive root (appr. 1.43756) of the cubic equation

$$\lambda^3 = \frac{1}{2}\lambda^2 + \lambda + \frac{1}{2}.$$

Here we study random (with equal probabilities) Fibonacci-Padovan sequences and consider a problem of visualization of the tree of possible outcomes. We represent elements of random sequences as triplets (x,y,z) and define operators $F(x,y,z) = (y,z,y+z)$ and $P(x,y,z) = (y,z,x+y)$ for Fibonacci and Padovan sequence correspondingly. To visualize individual random sequences we suggest direction-length attitude, where $length = (x+y+z), \quad direction = (x,y,z)/length$.

To visualize full set of possible outcomes, we use colour-brightness approach, where RGB colour and brightness correspond to direction-length. When studying probability distribution of all possible directions, it could be also useful to visualize directions only. Suggested algorithms are realized in Wolfram *Mathematica* 10.4.

If we use a triplet $(1,1,1)$ as a start, next triplet will be $(1,1,2)$ independent on what operator is used since $F(1,1,1) = P(1,1,1) = (1,1,2)$ (see right branch on Figure 1). So in our studies we use triplet $(1,1,2)$ as the starting point. The possible triplets may be written as $W(1,1,2)$ where $W \in < F,P >$, the set of words generated by F and P.

Let us note that

$$FPF(x,y,z) = FP(y,z,y+z) = F(z,y+z,y+z) = (y+z,y+z,2(y+z))$$

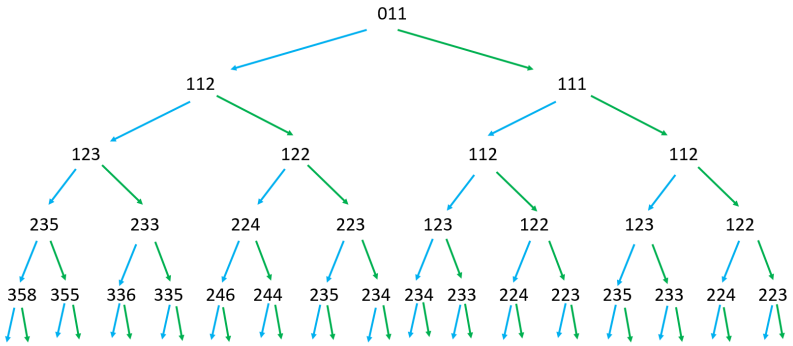


Figure 1: The Fibonacci-Padovan tree. Left (blue) arrow corresponds to Fibonacci operator applied, right (green) - Padovan.

which is a multiple of $(1,1,2)$. So, whenever the sequence FPF appears somewhere in the word W, we get a subtree similar to the full tree $W(1,1,2)$. Some nodes multiple of $(1,1,2)$ are highlited on Figure 2.

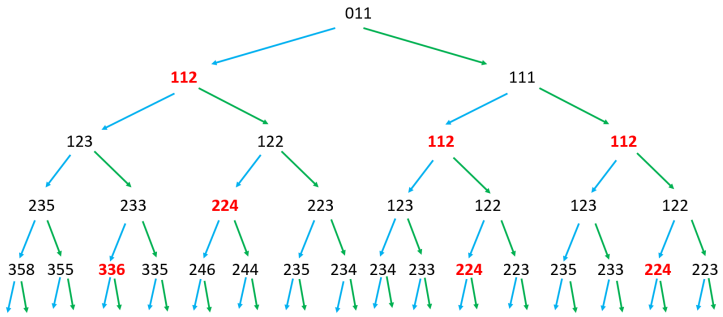


Figure 2: The Fibonacci-Padovan tree. Multiples of $(1,1,2)$ are marked red.

We characterise triplets (x,y,z) by direction and length, where

$$length = (x+y+z),$$

$$direction = (x,y,z)/length = (\frac{x}{x+y+z}, \frac{y}{x+y+z}, \frac{z}{x+y+z}).$$

This approach (to use directions, i.e. normalize components of the vector by its norm) was used, e.g., by Furstenberg and Kesten [5].

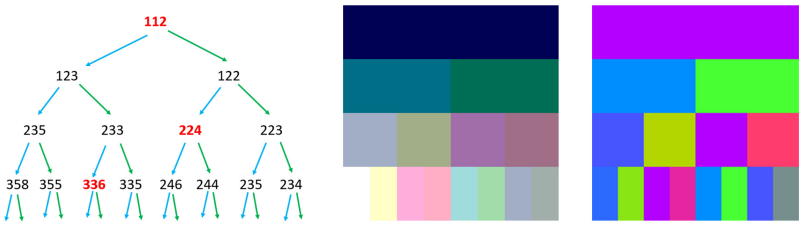


Figure 3: Part of the Fibonacci-Padovan tree (left) and its RGB visualizations: direction-length (center) and directions only (right).

Figure 3 shows first four levels of the tree and its RGB visualizations: direction-length (brightness is normalized by the last element of the largest triplet corresponding to the word $FFF\ldots$) and directions only. Figure 4 shows larger part of the tree.

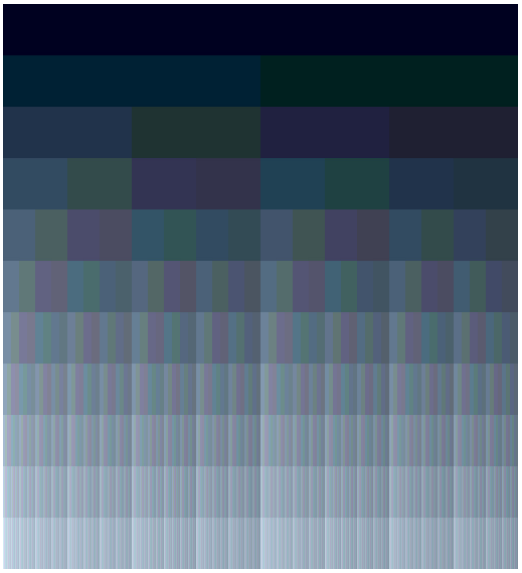


Figure 4: RGB visualization.

Let us note that operators $F(x,y,z) = (y,z,y+z)$ and $P(x,y,z) = (y,z,x+y)$ put some restrictions on the elements of triplets: for the triplet (x,y,z) we always have $x \leq y \leq z$ and $y \leq 2x$, $z \leq 2y$. It restricts the colors of the image. To improve

the situation one can add extra transformation of colours, the simplest is to use the command ImageAdjust in Wolfram Mathematica (see Figure 5).

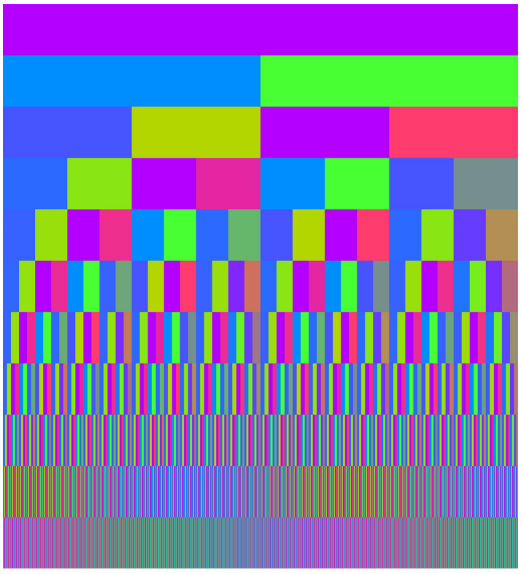


Figure 5: RGB visualization (directions only) with modified color space. Multiples of $(1,1,2)$ are easily seen - they have same color as the first (uppermost) stripe.

Interesting results could be obtained also if one uses HSB (hue-saturation-brightness) approach, see Figures 6 and 7.

References

[1] L. Pisano, *Liber Abaci* (1202).

[2] R. Padovan, *Dom Hans Van Der Laan and the Plastic Number*, in K. Williams and J. F. R. Fucecchio (eds.), Nexus IV: Architecture and Mathematics, Kim Williams Books, pp.181-193 (2002).

[3] D. Viswanath, *Random Fibonacci sequences and the number 1.13198824 . . .* , Mathematics of Computation **69**, 231, pp. 1131-1155 (1999).

[4] N. Gogin and A. Mylläri, *On the Average Growth Rate of Random Compositions of Fibonacci and Padovan Recurrences*, Lecture Notes in Computer Science **5743**, pp. 240-246 (2009).

[5] H. Furstenberg and H. Kesten, *Products of Random Matrices*, Ann. Math. Statist. **31**, 2, pp. 457-469 (1960).

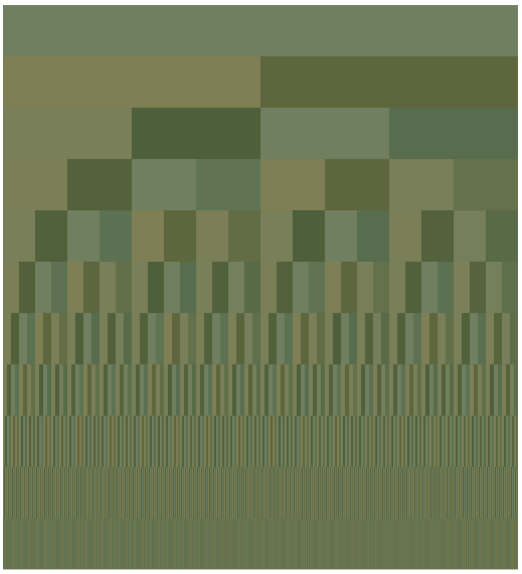


Figure 6: HSB visualization (directions only).

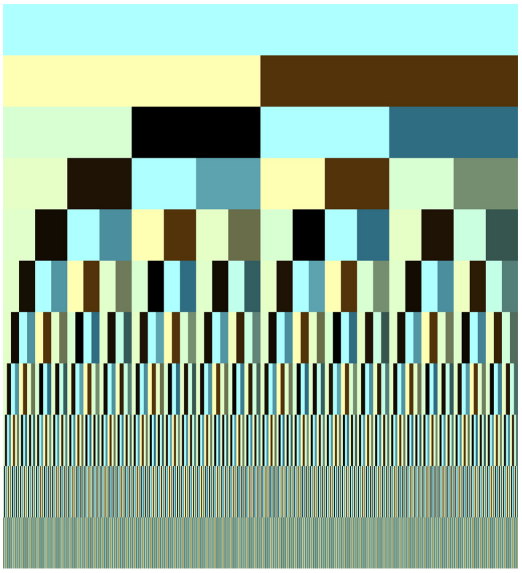


Figure 7: Same as Figure 6 with adjusted colours.

Symbolic Contour Integration in Mathematica (Part 2): Some Special Topics to be Investigated

Robert Kragler

Weingarten University of Applied Sciences, D-88241, Weingarten, Germany,
kragler@hs-weingarten.de

While the first part was devoted only to the main procedures calculateResidues and ContourIntegration applied to a wide class of complex functions $f(z)$ which are rational polynomials, products of rational and trigonometric/hyperbolic functions, rational functions consisting of trigonometric/hyperbolic functions. However, the investigations of the second part of this paper are special topics which occur in the context of contour integration and are of interest in itselves. The issues discussed in this paper are:
(1) introduction of a language for creation and visualization of non-trivial integration paths consisting of polylines and circular arcs such as contours γ which exclude certain poles or branch cuts, or the sophisticated contour for Meijer G-functions meandering around integer singularities but avoiding half-integral ones, or the Pochhammer double-loop contour for the evaluation of the so-called Euler's integral etc. ;
(2) criterium for the determination of poles inside/outside an arbitrary closed contour;
(3) visualization and extraction of (non-trivial) branch cuts for various functions $f(z)$ such as $\sqrt{\sin(z)}$ or $\arcsin(z^n)$;
(4) treatment of contour integrals for which the integrands possess branch cuts such as $f(z) = \sqrt{z}/(z^2+1)$;
(5) transformation of improper integrals (along the real axis) into exotic contour integrals with the help of change of variables, e.g. $\int_0^{+\infty} \frac{1}{x^3+1} dx$ with variables $x \to re^{i\Phi}$ where $\Phi \to \frac{2\pi}{3}$ etc.;
(6) symbolic evaluation of the integral representation for special functions such as Meijer G-function or Euler's integral for Beta function.

References

[1] R. Kragler, *Contour Integration: a Procedure still missing in Mathematica*, Lecture at XVII Mathematica-Tag, (18 Febr. 2016) WIAS/Berlin (2016).

[2] R. Kragler, *R. Kragler, Contour Integration - or what is still missing in Mathematica, Part1 : Residues and Contour Integration*, (2016), to be published.

[3] P. Wellin, *Programming with Mathematica, An Introduction*, Cambridge University Press, Chapt. 10.4, pp. 419 (2013).

[4] M. Trott/WRI, private communication (10/2013).

[5] E. W. Weisstein, *MathWorld* (2007), see: http://mathworld.wolfram.com/BranchCut.html and BranchCut.nb.

[6] Yu-Sung Chang, *Surface with Branch Cuts* from Wolfram Demonstrations Project, http://demonstrations.wolfram.com/SurfaceWithBranchCuts/.

[7] MathSource\0205-005 and MatheSource\0205-207.

[8] M. Rytin, *Integration across Branch Cuts*, MathSource 0212-409 (2002).

[9] S. Hassani, *Mathematical Physics; A Modern Introduction to Its Foundations*, Springer-Verlag, Chapt. 10.3.9, pp. 283-285 (1999).

[10] R. Gass, *Mathematica for Scientists ana Engineers: Using Mathematica to do Science*, Prentice Hall, Chap. 2.1.1, pp. 48-51 (1998).

[11] A. Sommerfeld, *Atombau und Spektrallinien*, Verlag Harri Deutsch, ISBN 3-87144-484-7, pp. 655 - 659 "Mathematische Zusätze und Ergänzungen", (4.) Ausführung einiger Integrale auf komplexem Wege. (1978) and L. Waldmann, *Quantentheorie Vorlesung*, WS 1965/66 University of Erlangen.

[12] H. Goldstein, C.P. Poole Jr. and J.L. Safko, *Classical Mechanics*, 3rd Ed. Pearson Education, Inc. , Chapt. 10.8, "The Kepler Problem in Action and Angle Variables", pp, 505-516 (2002).

[13] M. Trott/WRI, private communications (9/2013), and discussions in MathGroup: A. Krasnov [mg131613] and A. Elkins [mg131572].

[14] Youngjoo Chung, *MathGroup* [mg131582] with Mathematica package SymbolicComputing presented at WTC2011 (see https://symbcomp.gist.ac.kr). D. Park, *MathGroup* [mg131569] with Mathematica package Presentations`StudentsIntegral.

[15] E. W. Weisstein, *Meijer G-Function from MathWorld* (2008): http://mathworld.wolfram.com/MeijerG-Function.html and MeijerG-Function.nb

[16] M. Trott, *The Mathematica Guidebook for Symbolics*, Springer-Verlag, Solutions 7a, pp. 1245-1248 (2006) and private communication (9/2013).

[17] F.W.J. Oliver, D.W. Lozier, R.F. Boisvert and C.W. Clark, *NIST Handbook of Mathematical Functions*, Cambridge University Press , Chapt. 5.12, p. 142 (2010).

[18] M. Trott and O. Marichev, from The Wolfram Functions Site: http://functions.wolfram.com/NB/Notations.nb (description of the special contour $\mathscr{L}$).

[19] A. P. Prudnikov, Yu. A. Brychkov and O. I. Marichev, *Evaluation of Integrals and the Mellin Transform*, Itogi Nauki i Tekhniki, Seriya Matemat. Analiz, Vol. 27, pp. 3-146 (1998), and A.P. Prudnikov, O.I. Marichev and Yu.A. Brychkov, *Integrals and Series. Vol. 3 : More Special Functions*, Gordon and Breach, Chapt. 8.2: "The Meijer G-Function $G_{p,q}^{m,n}\left(z\left|{}^{(a_p)}_{(b_q)}\right.\right)$", pp. 617-626 (1990).

Motion of a Swinging Atwood's Machine: Simulation and Analysis

Alexander Prokopenya

Warsaw University of Life Sciences – SGGW, Warsaw, Poland,
Collegium Mazovia Innovative Higher School, Siedlce, Poland
alexander_prokopenya@sggw.pl

The Atwood machine is a well-known device that is usually used to demonstrate the uniformly accelerated motion (see Ref. [1]). It consists of two bodies attached to opposite ends of a massless inextensible thread wound round a massless frictionless pulley. It is assumed that each body can move only along a vertical, and the thread doesn't slip on the pulley. Such Atwood's machine is a simple mechanical system with one degree freedom and one can easily show that the bodies acceleration is given by

$$a = \frac{m_2 - m_1}{m_2 + m_1}\, g\ , \tag{1}$$

where m_1 and m_2 $(m_2 > m_1)$ are the bodies masses, and g is the gravity acceleration. As the acceleration a can be easily found experimentally Eq. (1) is often used to find the local Earth gravity constant g.

However, doing the corresponding experiment, one can observe that the result obtained may differ noticeably from the true value of g. Trying to explain such result, one can notice that it is very difficult to constrain the bodies to move strictly along verticals and to avoid their oscillations.

It should be noted that swinging Atwood's machine has been a subject of a number of papers (see, for example, Refs. [2, 3, 4, 5, 6]) and its mechanical behaviour has been studied quite well. In particular, it has been proven that the system of differential equations describing dynamics of swinging Atwood's machine is not integrable, in general. It has been shown also that, depending on the mass ratio m_2/m_1, the system can demonstrate different types of motion, namely, periodic, quasi-periodic, or chaotic motion but physical reasons of such behaviour of the system and significance of oscillations has not been usually discussed.

The main purpose of the present paper is to analyze the terms appearing in the equations of motion owing to oscillations and to study their influence on the system behaviour. Combining symbolic and numerical calculations turns out to be very useful for this study because the equations of motion are not integrable. The validity of the results obtained is demonstrated by means of the simulation of motion of the swinging Atwood machine with the computer algebra system Mathematica (see Ref. [7]) that is used for doing all relevant symbolic and numerical

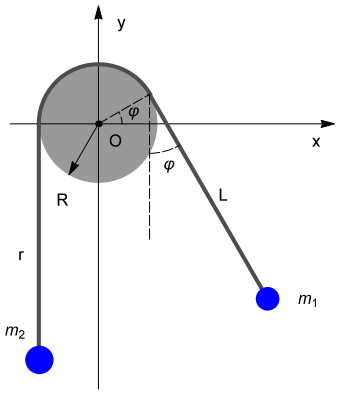


Figure 1: The swinging Atwood machine.

calculations and visualization of the results.

1 Equations of Motion

We consider here a generalized model of the simple Atwood machine when the body of mass m_1 is allowed to swing in a plane while the other body of mass m_2 is constrained to move along a vertical (see Fig. 1). Such a system has two degrees of freedom and its geometrical configuration can be described in terms of two variables, for example, an angle of the pulley rotation ψ, and an angle φ determining deviation of the thread from a vertical. Note that the length L of the thread between the body m_1 and the point, where the thread departs from pulley, is given by the relationship $L = L_0 + R(\varphi - \psi)$, where L_0 is its initial value, R is a radius of the pulley, and initial values of ψ and φ are assumed to be equal ($\psi_0 = \varphi_0$). Assuming the thread doesn't slip on the pulley, we obtain $r = r_0 + R(\psi - \psi_0)$, where r_0 is an initial length of the thread between the body m_2 and the pulley.

The Lagrangian of the system can be written in the form

$$\begin{aligned}\mathscr{L} = &\frac{1}{2} m_1 \left(L_0 + R(\varphi - \psi)\right)^2 \dot{\varphi}^2 + \frac{1}{2}\left(I_0 + (m_1 + m_2)R^2\right)\dot{\psi}^2 \\ &- m_1 g \left(R\sin\varphi - (L_0 + R(\varphi - \psi))\cos\varphi\right) + m_2 g R \psi \ , \end{aligned} \tag{2}$$

where the dot denotes differentiation with respect to time, and I_0 is a moment of inertia of the pulley. Using Eq. (2) and doing standard symbolic calculations, we obtain the equations of motion in the form

$$\ddot{\psi} = \frac{R}{I_0 + (m_1 + m_2)R^2}\left(g(m_2 - m_1\cos\varphi) - m_1(L_0 + R(\varphi - \psi))\dot{\varphi}^2\right) \ , \tag{3}$$

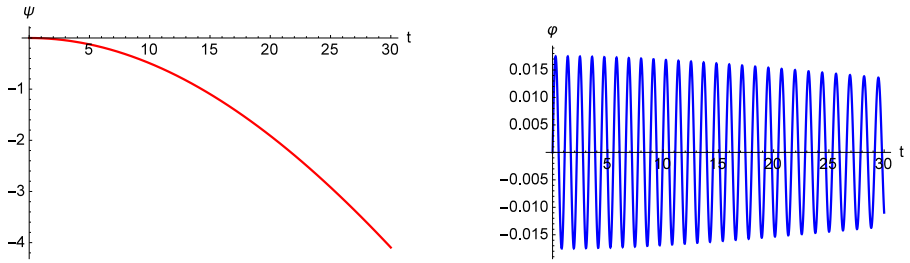


Figure 2: Motion of the swinging Atwood machine in case of $m_1 = m_2$.

$$\ddot{\varphi} = \frac{1}{L_0 + R(\varphi - \psi)} \left(2R\dot{\psi}\dot{\varphi} - g\sin\varphi - R\dot{\varphi}^2\right) . \tag{4}$$

One can readily see that in case of absence of oscillations, when $\varphi \equiv 0$, Eq. (4) is satisfied identically, while Eq. (3) takes the form

$$\ddot{\psi} = \frac{gR(m_2 - m_1)}{I_0 + (m_1 + m_2)R^2} . \tag{5}$$

Obviously, it determines the uniformly accelerated motion of the system and generalizes Eq. (1) to the case of nonzero mass of the pulley.

2 Main results

Taking into account planar oscillations of the body m_1 complicates the equations of motion significantly (see Eqs. (3)-(4)) and their general solution cannot be found in an analytical form. However, choosing some realistic values of the system parameters, we can find the corresponding numerical solution for different initial conditions and to get some ideas on possible motion of the system.

At first we consider the case of equal masses ($m_1 = m_2$) and assume that the bodies are at rest. As a vertical initial velocity of the bodies induces only their uniformly accelerated motion without oscillations we give the body m_1 a small initial velocity in a horizontal direction. Due to the fact that both bodies have the same mass and are initially in equilibrium, it seems to be quite natural to assume that the system should move in the neighborhood of its equilibrium position. However, this equilibrium position turns out to be unstable and the system moves away from the equilibrium even for very small values of initial velocity.

Actually, solving Eqs. (3)-(4)) with the initial conditions $\psi(0) = \dot{\psi}(0) = \varphi(0) = 0$, $\dot{\varphi}(0) = 0.1$, we obtain a solution shown in Fig. 2. One can readily see that arising oscillation of body m_1 results in a clockwise rotation of the pulley and movement

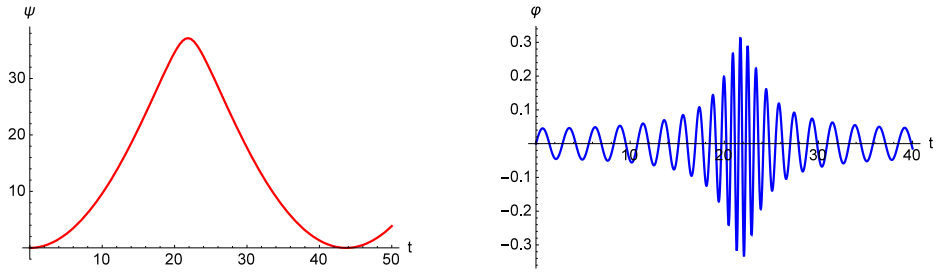


Figure 3: Motion of the swinging Atwood machine in case of $m_1 < m_2$.

of the bodies in vertical direction. Amplitude of oscillation decreases with time and the term in the right-hand side of Eq. (3) tends to zero as it should be in case of the absence of oscillation and equal masses of the bodies. Thus, due to oscillation of the body m_1 a transformation of its initial horizontal momentum into vertical motion of the bodies takes place. A physical reason of such transformation is an increase of a tension of the thread due to oscillation of the body m_1 and appearance of the centrifugal force $m_1 L\dot{\varphi}^2$. Computing an average value of the net force in the right-hand side of Eq. (3) shows that it really becomes smaller than zero when body m_1 oscillates, in spite of the equal masses of the bodies.

Note that the thread tension depends on amplitude of the body m_1 oscillation. If the amplitude is quite small and the mass of body m_2 is greater than mass m_1 the net force in the right-hand side of Eq. (3) may become positive. Then the pulley starts to rotate counterclockwise and the thread length L between the body m_1 and pulley decreases. The amplitude of oscillation and the thread tension starts to grow up and if the masses difference $m_2 - m_1$ is less than some critical value the net force in the right-hand side of Eq. (3) becomes negative again. As a result angular velocity $\dot{\psi}$ of the pulley changes the sign and the system starts to move in opposite direction. Then amplitude of oscillation decreases again and when its value becomes small enough angular velocity $\dot{\psi}$ changes the sign and the process repeats. Thus, we can observe a quasi-periodic motion of the swinging Atwood machine (see Fig. 3). This result is quite unexpected and it should be taken into account when the Atwood machine is used for measuring the gravity acceleration.

3 Conclusions

In the present talk we have analyzed an influence of oscillation on the Atwood machine motion in the simplest case when only one body is permitted to oscillate in a plane. Nevertheless, we have shown that even such oscillation can completely

modify a motion of the system, while the simple Atwood machine demonstrates only the uniformly accelerated motion of the bodies. Of course, a mass and size of the pulley and changing the length L between the body m_1 and pulley owing to winding the thread on the pulley affect on the system motion, as well. Doing necessary calculation, we have shown that these factors only change an inertness of the system and modify oscillation of the body m_1 but do not change qualitatively the system behaviour.

It should be noted that there are many physical problems which seem to be quite simple although the corresponding mathematical models are rather complicated to be solved and analyzed by hand. But application of the modern computer algebra systems such as Wolfram Mathematica, for example, helps a lot in analyzing such problems and promotes development of physical intuition and better understanding of the subject.

References

[1] G. Atwood, *A Treatisa on the Rectilinear Motion and Rotation of Bodies*, Cambridge University Press (1784).

[2] N.B. Tufillaro, T.A. Abbott, D.J. Griffiths, *Swinging Atwood's machine*, Amer. J. Phys. **52**, pp. 895-903 (1984).

[3] N.B. Tufillaro, *Motions of a swinging Atwood's machine*, J. Physique **46**, pp. 1495-1500 (1985).

[4] J. Casasayas, T.A. Nunes, N.B. Tufillaro, *Swinging Atwood's machine: integrability and dynamics*, J. Physique **51**, pp. 1693-1702 (1990).

[5] H.M. Yehia, *On the integrability of the motion of a heavy particle on a tilted cone and the swinging Atwood's machine*, Mech. R. Comm. **33**, 5, pp. 711-716 (2006).

[6] O.Pujol, J.P. Pérez, J.P. Ramis, C. Simo, S. Simon, J.A. Weil, *Swinging Atwood machine: Experimental and numerical results, and a theoretical study*, Physica D, **239**, 12, pp. 1067-1081 (2010).

[7] S. Wolfram, *The Mathematica Book*, 5th ed., Wolfram Media (2003).

Construction of Analytical Solutions to Nonlinear Evolution Equations Using the Generalized Differential Operator Method

T. Telksnys[1], Z. Navickas[1], M. Ragulskis[1],

[1] *Kaunas University of Technology, Department of Mathematical Modeling, Lithuania, tadas.telksnys@ktu.edu, zenonas.navickas@ktu.lt, minvydas.ragulskis@ktu.lt*

There are a number of mathematical tools which, with the help of computer algebra, provide powerful techniques for the solution of nonlinear evolutions in mathematical physics. The generalized differential operator method, first introduced in [1], has been successfully applied for the construction of solitary solutions to equations in mathematical physics [2, 3]. In this talk, we consider the use of this method to construct more general closed-form analytical solutions.

Since the wave variable substitution $x = \xi - at$ transforms nonlinear evolution equations into ordinary differential equations, we consider the following initial value problem:

$$y''_{xx} = P\left(x, y, y'_x\right); \quad y = y(x;c,s,t), \quad y(c;c,s,t) = s, \quad y'_x(c;c,s,t) = t. \qquad (1)$$

The generalized differential operator for (1) reads $\mathrm{D} := \mathrm{D}_c + t\mathrm{D}_s + P(c,s,t)\mathrm{D}_t$. Denoting $p_j(c,s,t) := \mathrm{D}^j s$, the general solution to (1) can be expressed as the series $y = y(x;c,s,t) = \sum_{j=1}^{+\infty} \frac{(x-c)^j}{j!} p_j(c,s,t)$. We show that if $f(x) = \sum_{j=1}^{+\infty} \frac{q_j}{j!} x^j$ is an arbitrary analytical function and the sequence $\widehat{p}_j = \frac{p_j}{q_j}$ is a linear recurring sequence of order n [4], the solution to (1) can be written in closed form as $y = \sum_{k=1}^{n} \lambda_k f\left(\alpha_k - \beta_k (x-c)\right)$, where $\lambda_k, \alpha_k, \beta_k \in R$ are constants.

The outlined algorithm is a powerful tool for the construction of closed-form solutions to nonlinear evolution equations in mathematical physics.

References

[1] Z. Navickas, L. Bikulciene, *Expressions of solutions of ordinary differential equations by standard functions*, Math. Model. Anal. **11**, pp. 399-412 (2006).

[2] Z. Navickas, L. Bikulciene, M. Ragulskis, *Generalization of Exp-function and other standard function methods*, Appl. Math. Comput. **216**, pp. 2380-2393 (2010).

[3] Z. Navickas, L. Bikulciene, M. Rahula, M. Ragulskis, *Algebraic operator method for the construction of solitary solutions to nonlinear differential equations*, Commun. Nonlinear Sci. Numer. Simulat. **18**, pp. 1374-1389 (2013).

[4] V. L. Kurakin, A. S. Kuzmin, A. V. Mikhavel, A. A. Nechaev, *Linear recurring sequences over rings and modules*, J. Math. Sc. **76**, pp. 2793-2915 (1995).

On Degenerate Central Configurations in the N-Body Problem

Agnieszka Siluszyk

Siedlce University of Natural Sciences and Humanities, Faculty of Science, Poland
agnieszka.siluszyk@uph.edu.pl

The existence of central configurations in the N-body problem is connected with two type of parameters, masses of the bodies, which are physical parameters, and positions of the bodies as geometrical parameters. The main goal concerning central configurations is to determine the values (m_i, q_i), $i = 1, \ldots, N$ of the parameters for which such arrangement of the N point masses exists. The well known list of classical central configurations of Euler and Lagrange has been completed by B. Elmabsout [1]. He has added a configuration consisting of $2n$ equal point masses, located at the vertices of two regular concentric n-gons, while the point mass with nonzero mass m_0 lies in the center of these polygons. He has proved that such configuration exists if and only if these two polygons are homothetic, or differ by an angle of π/n.

The bifurcation's problem is the second one which is connected with the degenerate central configurations and for which lots of interesting questions arise. The authors which have dealed with bifurcations in the n-body problem are M.Sekiguchi [4] and J.Lei, M.Santoprete [5]. They have analyzed a highly symmetrical *rosette configuration* of $2n+1$ point masses; Sekiguchi has considered $2n$ point masses with mass m situated at the vertices of two different coplanar and concentric regular n-gons, whilst Lei, Santoprete have analized $2n$ point masses, for which n particles with m_1 mass are located at the vertices of n-gon and n particles with the mass m_2 lie at the vertices of another n-gon. Both n-gons are regular, concentric and rotated of an angle $\frac{\pi}{n}$. The mass m_0 lies at the center of masses. Sekiguchi has established that if $n \geq 3$ and $\mu < \mu_c$, where the parameter μ controls bifurcations, then there exist three central configurations, otherwise only one for $\mu \geq \mu_c$. J.Lei and M.Santoprete have shown that if $n \geq 3$ then there exists a degenerate central configuration and a bifurcation for value of the parameters μ, ε.

Assume that $m_j \in R^+$ $(j = 1, ..., N)$ and $q \neq q'$ are distinct radii of two concentric regular polygons. We deal with a new class of central configurations in the N-body problem. By $(2,N)$ we understand the configuration which consists of n point masses $m_1, m_2, \ldots, m_n$ situated at the vertices of the regular n-gon, and of $2n$ point masses $m_1', m_2', \ldots, m_{2n}'$ located at the vertices of the regular $(2n)$-gon, so, $N = 3n$.

The existence of such configuration has been shown numericaly by E.A.

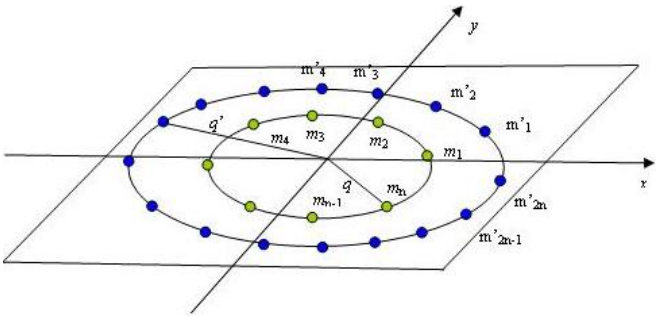


Figure 1. Configuration $(2,N)$.

Grebenikov [2] and has been established in the case $n = 2$ by A. Siluszyk [3]. In our work we deal with a family of central configurations of n point masses, when $n = 2$. If there exists a constant λ such that [6]

$$m^{-1}\frac{\partial U}{\partial \rho} = \lambda \rho, \tag{1}$$

then the configuration $\rho = (q_1, q_2, \ldots, q_N) \in \left\{R^2 \setminus \Delta\right\}$ is called a *central configuration* in the N-body problem; here $U = \sum_{1\le i<j\le N} \frac{m_i m_j}{r_{ij}}$, $r_{ij} = \left|q_j - q_i\right|$, $\Delta = \left\{\rho : q_i = q_j, i \neq j\right\}$ and $m = diag\,[m_1, m_2, \ldots, m_N]$. Any central configuration gives *relative equilibrium* which rotates in the plane with constant angular velocity ω and remains congruent to itself for all times. We assume that $\sum_{i=1}^{N} m_i q_i = 0$, i.e., the center of mass of our system is located at the origin, moreover, we know [6] that $\lambda = \frac{U(\rho)}{I(\rho)}$, where $I(\rho) = \rho^T m \rho$ means the moment of inertia. The set of equivalence classes of central configurations are determined by critical points of $U(\rho)|_X$, where $X = \left\{R^2 \setminus \Delta : I(\rho) = 1\right\}$, $I = \sum_{i=1}^{N} m_i q_i^2$ [7]. Moreover the critical points which are degenerated, i.e. the Hessian $D^2(U(\rho)|_X)$ at such points has a nontrivial nullspace, give us an equivalence class of degenerated central configurations.

We deal with configuration of the type $(2,N)$ with any natural N and $m_1, m_2, m_3 > 0$, $q, q' > 0$. Then we have:

Theorem 1. ([3]) For any natural N and any real numbers $m_1 > 0$, and q, $r > 0$ $(r = \frac{q'}{q})$ a central configuration of type $(2,N)$ exists if and only if

$$\left\{\begin{array}{rcl} m_2 & = & \frac{r^2}{(\kappa_1-\kappa_6)(\kappa_1-4r^3(\kappa_2+\kappa_4)+4r^4(\kappa_3+\kappa_5)+\kappa_6)}(-16r^5(\kappa_2-\kappa_4)\kappa_5+ \\ & & +16r^4(\kappa_2\kappa_4-\kappa_4^2+\kappa_5(\kappa_3-\kappa_5))-16r^3\kappa_4(\kappa_3-\kappa_5)+ \\ & & -r(-\kappa_1^2-4\kappa_4\kappa_6+\kappa_1(4\kappa_2+\kappa_6))+4\kappa_1\kappa_3-4\kappa_5\kappa_6)m_1, \\ m_3 & = & \frac{r^2}{(\kappa_1-\kappa_6)(\kappa_1-4r^3(\kappa_2+\kappa_4)+4r^4(\kappa_3+\kappa_5)+\kappa_6)}(16r^5\kappa_3(\kappa_2-\kappa_4)+ \\ & & -16r^4(\kappa 2(\kappa 2-\kappa_4)+\kappa_3(\kappa_3-\kappa_5))+16r^3\kappa_2(\kappa_3-\kappa_5)+ \\ & & +r(\kappa_1(\kappa_1-4\kappa_4-\kappa_6)+4\kappa_2\kappa_6)+4(\kappa_1\kappa_5-\kappa_3\kappa_6))m_1, \end{array}\right. \tag{2}$$

(here, the sums in the right hand side do not depend on k). The elements κ_s, $s = 1,..,6$ for any $k = 1,\ldots,n$ are expressed by [3]:

$$\left\{\begin{array}{rcl}
\kappa_1 & = & \sum\limits_{j=1}^{n} \frac{1}{\left|\sin\frac{\pi(k-j)}{n}\right|}, \\
\kappa_2 & = & \sum\limits_{j=1}^{n} \frac{1}{(1+r^2-2r\cos(\frac{2\pi(j-k)}{n}+\frac{\pi}{n}))^{\frac{3}{2}}}, \\
\kappa_3 & = & \sum\limits_{j=1}^{n} \frac{\cos(\frac{2\pi(j-k)}{n}+\frac{\pi}{n})}{(1+r^2-2r\cos(\frac{2\pi(j-k)}{n}+\frac{\pi}{n}))^{\frac{3}{2}}}, \\
\kappa_4 & = & \sum\limits_{j=1}^{n} \frac{1}{(1+r^2-2r\cos(\frac{2\pi(j-k)}{n}+\frac{2\pi}{n}))^{\frac{3}{2}}}, \\
\kappa_5 & = & \sum\limits_{j=1}^{n} \frac{\cos(\frac{2\pi(j-k)}{n}+\frac{2\pi}{n})}{(1+r^2-2r\cos(\frac{2\pi(j-k)}{n}+\frac{2\pi}{n}))^{\frac{3}{2}}}, \\
\kappa_6 & = & \sum\limits_{j=1}^{n} \frac{1}{\left|\sin(\frac{2\pi(j-k)}{2n}+\frac{\pi}{2n})\right|}.
\end{array}\right. \tag{3}$$

Here, we consider the relative equilibrium of six bodies; such configuration consists of (m_i, q_i), $i = 1,...,6$ point masses, two of them with equal masses m_1 situated at the ends of a segment having lenght $2q$, while other two pairs of masses m_2 and m_3 are located at the vertices of a square whose side is $q'\sqrt{2}$. Moreover, the vertices of this square are on the axises of symmetry of the segment. The Newtonian potential and the moment of inertia for the configuration of the type $(2,6)$ are given by:

$$\left\{\begin{array}{rcl}
U & = & \frac{m_1^2}{q}((\frac{1}{2}+\frac{\mu^2+\nu^2}{2r})+4\frac{\mu}{\sqrt{1+r^2}}+2\nu(\frac{1}{\sqrt{(r-1)^2}}+\frac{1}{\sqrt{(r+1)^2}})+2\sqrt{2}\frac{\mu\nu}{r}), \\
I & = & 2m_1q^2(1+r^2(\mu+\nu)).
\end{array}\right. \tag{4}$$

for parameters $\mu = \frac{m_2}{m_1} > 0$ and $\nu = \frac{m_3}{m_1} > 0$, $r = \frac{q'}{q}$.

Theorem 2. Suppose, that $(2,6)$ is configuration of six bodies with $q, q' > 0$ as mutual distances corresponding to $|Om_1|$, $|Om_2| = |Om_3|$, respectively. Then for all $m_1, m_2, m_3 > 0$ there exists at least one central configuration of the type $(2,6)$.

Solving the equation $\nabla U(\rho) + \frac{1}{2}\sigma\nabla I(\rho) = 0$ with respect to unknown q, r from (4), we obtain in the plane $I = 1$ the equation $U_r' \cdot I_q' - U_q' \cdot I_r' = 0$. The solutions of this equation give us all central configurations of the $(2,6)$.

Proposition 1. For any $m_1 > 0$ there exists at least one r^* for which the configuration of the type $(2,6)$ is the equivalence class of a degenerated central configuration.

Computer Assisted Proof methods are applied to obtain the main results of our report. These methods represent a new technique for obtaining rigorous results

concerning the global dynamics of nonlinear systems of the equations (see, e.g., P. Zgliczynski [8]). Below we present the number of critical points for r^* and critical masses μ^*, ν^* (here, we put $m_1 = 0.001$):

r^*	critical masses μ^*, ν^*	number of c.p.
0.70582611533?	$\mu^* = 58.38984663223665?$, $\nu^* = 0.944757994652664?$	8
0.6226157?	$\mu^* = 30.07078175550046?$, $\nu^* = 2.359914736266285?$	12
0.5025690268698576?	$\mu^* = 3.18858 * 10^{13}$, $\nu^* = 3.18858 * 10^{13}$	14
0.5646596968686869?	$\mu^* = 22.45513293937953?$, $\nu^* = 5.061034347849054?$	16
9.3445?	$\mu^* = 15.117653893458127?$, $\nu^* = 0.017734428734047708?$	20

Table 1: Number of critical points for given distances r^* and masses μ^*, ν^*.

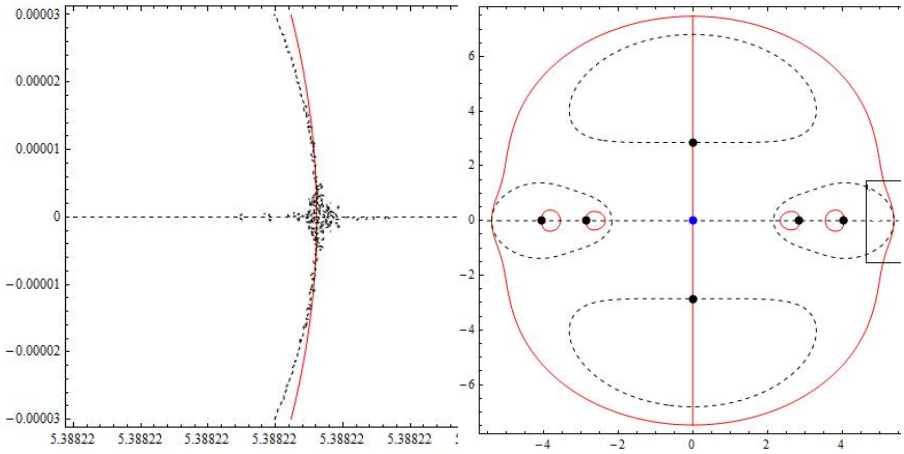


Figure 2. The degenerate central configuration for $r^* = 0.70582611533?$, $\mu^* = 58.38984663223665?$ and $\nu^* = 0.944757994652664?$.

The change which is presented by Table 1 and Figure 2 expresses an exchange of the number of solutions 16 for 8, 12, 14 and 20 in the equation $U_r' \cdot I_q' - U_q' \cdot I_r' = 0$.

In our studies we apply a few theoretical facts concerning interval arithmetic. Using a theorem and some methods it is possible to find rigorous bounds on roots of nonlinear equation. We use Sage arbitrary precision real intervals, in which an

interval $[a,b]$ is written as a standard floating-point number with a question mark, where question mark can be interpreted as an error.

References

[1] B. Elmabsout, *Nouvelles configurations d'equilibre relatif pour le probleme des N corps*, C. R. Acad. Sci. **329**, Serie II, pp. 467-472(1991).

[2] E. A. Grebenikov, *Mathematical Problems of Homographic Dynamics*, MAKS Press, Moscow, 2010.

[3] A. Siluszyk, *A new central configuration in the planar N-body problem*, CARPATHIAN J.MATH. **30**, No.3, pp. 401-408 (2014).

[4] M. Sekiguchi, *Bifurcation of central configuration in the* $2n+1$ *body problem*, Celestial Mechanics and Dynamical Astronomy **90**, pp.355-360, 2004.

[5] J. Lei, M. Santoprete, *Rosette Central Configurations, degenerate central configurations and bifurcations*, Celestial Mechanics and Dynamical Astronomy **94**, Issue 3, pp. 271-287, (2006).

[6] A. Wintner, *The Analytical Foundations of Celestial Mechanics*, Princeton University Press, 1941.

[7] J. Llibre, R. Moeckel, C. Simo, *Central Configurations, Periodic Orbits, and Hamiltonian Systems*, Springer Basel, 2015.

[8] P. Zgliczynski *Steady states bifurcations for theKuramoto-Sivashinsky equation - a computer assisted proof , a file with numerical data bifdata.txt* , Journal of Computational Dynamics, **2**, 95–142 2015.

Secular Perturbations in the Two-Planetary Three-Body Problem with the Masses Varying Anisotropically with Different Rates

M.Zh. Minglibayev[1,2], A.N. Prokopenya[3], G.M. Mayemerova[1], Zh.U. Imanova[1]

[1] *al-Farabi Kazakh National University, Almaty, Kazakhstan, mayemerova@gmail.com*
[2] *Fessenkov Astrophysical Institute, Almaty, Kazakhstan, minglibayev@mail.ru*
[3] *Warsaw University of Life Sciences, Warsaw, Poland, alexander_prokopen@sggw.pl*

1 Statement of the problem

Let us consider a system of three mutually attracting spherical celestial bodies T_0, T_1 and T_2 of masses

$$m_0 = m_0(t), \quad m_1 = m_1(t), \quad m_2 = m_2(t) \tag{1}$$

varying anisotropically with different rates (law of masses variation is arbitrary) (Refs. [1])

$$\frac{\dot{m}_0}{m_0} \neq \frac{\dot{m}_1}{m_1} \neq \frac{\dot{m}_2}{m_2}. \tag{2}$$

On the basis of Meshcherskiy equation (Refs. [2]), we can write the equations of motion of three-body problem with variable masses in the presence of reactive forces in the absolute coordinate system in the form

$$m_j\ddot{\vec{R}}_j = grad_{\vec{R}_j} U + \dot{m}_j\vec{V}_j, \quad U = f\left(\frac{m_0m_1}{R^*_{01}} + \frac{m_0m_2}{R^*_{02}} + \frac{m_1m_2}{R^*_{12}}\right),$$

where $\vec{u}_j$ are the absolute velocities of the separating particles,

$$\vec{V}_j = \vec{u}_j - \dot{\vec{R}}_j \neq 0, \quad j = 0, 1, 2, \tag{3}$$

are the relative velocities of the separating particles, $\vec{R}_j$ are the radius vectors of the center of the spherical bodies, $\vec{R}_{ij}$ are the distances between the centers of the spherical bodies, f is the gravitational constant. Following L.G. Lukyanov (Refs. [3]), we assume that the reactive forces are applied to the center of the respective spherical bodies. Usually in the observational astronomy the laws of the mass change (see Eqs. (1, 2)) and the relative velocities of the separating particles (see Eqs. (3)) can be determined experimentally for specific celestial bodies. Therefore, we assume that the values of $m_j(t)$, $\vec{V}_j$, $j = 0, 1, 2$, are known (see Eqs. (1, 3)).

It should be noted that in general case of the three-body problem with variable masses changing anisotropically in the different rates there is no any integral of motion. Therefore, the problem under consideration is investigated by methods of the perturbation theory (Refs. [1], [4, 5, 6]), and with the use of analytical calculations system Mathematica (Refs. [7]).

2 Equations of Motion in Terms of the Delaunay Elements

Using the Jacobi coordinates, we can rewrite the equations of motion in the form

$$\mu_1 \ddot{\vec{r}}_1 = grad_{\vec{r}_1} U + \vec{F}_1, \quad \mu_2 \ddot{\vec{r}}_2 = grad_{\vec{r}_2} U - (2\dot{\nu}_1 \dot{\vec{r}}_1 + \ddot{\nu}_1 \vec{r}_1) + \vec{F}_2.$$

where reduced masses are given by

$$\mu_1 = \frac{m_1 m_0}{m_0 + m_1} \neq const, \quad \mu_2 = \frac{m_2(m_0 + m_1)}{m_0 + m_1 + m_2} \neq const, \quad \nu_1 = \frac{m_1}{m_0 + m_1} \neq const.$$

The functions

$$\vec{F}_1 = \vec{F}_1(F_{1x}, F_{1y}, F_{1z}) = \vec{F}_1(t) = \frac{\dot{m}_1}{m_1}\vec{V}_1 - \frac{\dot{m}_0}{m_0}\vec{V}_0 \neq 0,$$

$$\vec{F}_2 = \vec{F}_2(F_{2x}, F_{2y}, F_{2z}) = \vec{F}_2(t) = \left(\frac{\dot{m}_2}{m_2}\vec{V}_2 - \frac{\dot{m}_0}{m_0}\vec{V}_0\right) - \nu_1 \left(\frac{\dot{m}_1}{m_1}\vec{V}_1 - \frac{\dot{m}_0}{m_0}\vec{V}_0\right) \neq 0,$$

are considered known and given.

To apply the perturbation theory it is convenient to rewrite the equations of motion in terms of the analogues of the second system of the Poincare elements. The first step in such transformation is to write the equations of motion in terms of the osculating elements of the aperiodic motion on the quasi-conic section using the Delaunay coordinates (see Refs. [4]). Then investigation of the secular perturbations of the Delanay elements is reduced to solving the following system of non-autonomous differential equations

$$\begin{aligned} \dot{\xi}_i &= \frac{\partial R^*_{isec}}{\partial \eta_i}, & \dot{p}_i &= \frac{\partial R^*_{isec}}{\partial q_i}, \\ \dot{\eta}_i &= -\frac{\partial R^*_{isec}}{\partial \xi_i}, & \dot{q}_i &= -\frac{\partial R^*_{isec}}{\partial p_i}. \end{aligned} \tag{4}$$

where R^*_{isec} are perturbation functions (Refs. [4, 5, 6]), ξ_i, η_i, p_i, q_i are analogues of the second system of the Poincaré elements (Refs. [1]).

In the present paper we consider the expansion of the perturbing function in terms of small quantities $m_1, m_2, e_1, e_2, i_1, i_2$ up to the second order inclusively (Refs. [4, 5, 6]). Then the secular expressions for R^*_{1sec}, R^*_{2sec} in the analogues of the second system of the Poincaré elements take the form (Refs. [5, 6])

$$\begin{aligned} R^*_{1sec} &= \frac{1}{\gamma_1^2}\cdot\frac{\tilde{\beta}_1^4}{2\mu_{10}\Lambda_1^2} + F_{01} + F_{12sec1} + F_{\rho 1sec} + \Phi_{1sec}, \\ R^*_{2sec} &= \frac{1}{\gamma_2^2}\cdot\frac{\tilde{\beta}_2^4}{2\mu_{20}\Lambda_2^2} + F_{02} + F_{12sec2} + F_{\rho 2sec} + V_{sec} + \Phi_{2sec}, \end{aligned} \tag{5}$$

$$F_{01} = -\frac{b_1\gamma_1^2 a_1^2}{2\psi_1} - f\frac{m_1 m_2}{\gamma_2\psi_1 a_2}, \quad F_{12sec1} = \frac{f}{\psi_1}\left[\frac{m_1 m_2}{r_{12}}\right]_{sec}, \quad F_{\rho 1sec} = -\frac{3b_1\gamma_1^2 a_1^2}{4\Lambda_1\psi_1}(\xi_1^2+\eta_1^2),$$

$$F_{02} = -\frac{b_2\gamma_2^2 a_2^2}{2\psi_2} - f\frac{m_1 m_2}{\gamma_2\psi_2 a_2}, \quad F_{12sec2} = \frac{f}{\psi_2}\left[\frac{m_1 m_2}{r_{12}}\right]_{sec}, \quad F_{\rho 2sec} = -\frac{3b_2\gamma_2^2 a_2^2}{4\Lambda_2\psi_2}(\xi_2^2+\eta_2^2),$$

$$V_{sec} = -\frac{9a_1 a_2\mu_2\gamma_2(2\dot{\gamma}_1\dot{\nu}_1+\gamma_1\ddot{\nu}_1)}{14\sqrt{\Lambda_1}\sqrt{\Lambda_2}\psi_2}(\xi_1\xi_2+\eta_1\eta_2),$$

$$\Phi_{1sec} = \frac{3a_1\gamma_1(t)}{2\psi_1\sqrt{\Lambda_1}}\left\{-F_{1x}(t)\xi_1 + F_{1y}(t)\eta_1 + \frac{F_{1z}(t)}{\sqrt{\Lambda_1}}\left[(-\xi_1 q_1 + \eta_1 p_1)\right]\right\},$$

$$\Phi_{2sec} = \frac{3a_2\gamma_2(t)}{2\psi_2\sqrt{\Lambda_2}}\left\{-F_{2x}(t)\xi_2 + F_{2y}(t)\eta_2 + \frac{F_{2z}(t)}{\sqrt{\Lambda_2}}\left[(-\xi_2 q_2 + \eta_2 p_2)\right]\right\}.$$

Analysis of the expressions obtained (see Eqs. (4, 5)) shows that the equations of the secular perturbations in the presence of reactive forces (in the case when masses changing anisotropically) are not splitted into two systems with respect to the elements ξ_i, η_i and p_i, q_i.

The main purpose of this paper is to identify the explicit form of the equations (see Eqs. (4)) and to find their approximate analytical solutions using by Picard method. On the basis of these solutions we can obtain an explicit form of the equations of the analogues of the orbital elements.

3 Approximate Analytical Solutions

Using expressions (5), we can write the equations of motion in explicit form (see Eqs. (4))

$$\begin{aligned} \dot{\xi}_1 &= K_5 + K_6 p_1 + 2K_1\eta_1 + K_3\eta_2, \quad \dot{\eta}_1 = K_4 - K_6 q_1 + 2K_1\xi_1 + K_3\xi_2, \\ \dot{\xi}_2 &= K_5' + K_6' p_2 + 2K_2'\eta_2 + K_3'\eta_1, \quad \dot{\eta}_2 = K_4' - K_6' q_2 + 2K_2'\xi_2 + K_3'\xi_1, \end{aligned} \tag{6}$$

$$\dot{p}_1 = -K_6\xi_1 + 2\psi_1^*(t)\left(\frac{q_1}{\Lambda_1} - \frac{q_2}{\sqrt{\Lambda_1\Lambda_2}}\right), \quad \dot{q}_1 = K_6\eta_1 + 2\psi_1^*(t)\left(\frac{p_1}{\Lambda_1} - \frac{p_2}{\sqrt{\Lambda_1\Lambda_2}}\right),$$
$$\dot{p}_2 = -K_6'\xi_2 + 2\psi_2^*(t)\left(\frac{q_2}{\Lambda_2} - \frac{q_1}{\sqrt{\Lambda_1\Lambda_2}}\right), \quad \dot{q}_2 = K_6'\eta_2 + 2\psi_2^*(t)\left(\frac{p_2}{\Lambda_2} - \frac{p_1}{\sqrt{\Lambda_1\Lambda_2}}\right). \tag{7}$$

In this formulation due to the anisotropical change of the masses and therefore adding of the reactive force new terms appear which have the form

$$K_4 = -\frac{3a_1F_{1x}(t)\gamma_1(t)}{2\psi_1\sqrt{\Lambda_1}}, \quad K_5 = \frac{3a_1F_{1y}(t)\gamma_1(t)}{2\psi_1\sqrt{\Lambda_1}} \quad K_6 = \frac{3a_1F_{1z}(t)\gamma_1(t)}{2\psi_1\Lambda_1},$$
$$K_4' = -\frac{3a_2F_{2x}(t)\gamma_2(t)}{2\psi_2\sqrt{\Lambda_2}}, \quad K_5' = \frac{3a_2F_{2y}(t)\gamma_2(t)}{2\psi_2\sqrt{\Lambda_2}} \quad K_6' = \frac{3a_2F_{2z}(t)\gamma_2(t)}{2\psi_2\Lambda_2},$$

and the values $K_1, K_2, K_3, K_1', K_2', K_3'$ were obtained in (Refs. [6]).

Using the method of Picard we can write the solutions of the equations (see Eqs. (6, 7)) as follows

$$\ni_k(t) = \ni_k(t_0) + \int_{t_0}^{t} \Pi_i^{**}(t, \ni_k(t_0))dt, \tag{8}$$

where $\Pi_i^{**}(t, \ni_k)$ are the right-hand sides of the equations (see Eqs. (6, 7)), $\ni_k$ are the elements ξ_i, η_i, p_i, q_i, and $\ni_{k0} = \ni_k(t_0)$ are their values at the initial time.

The solutions (see Eqs. (8)) allow to analyze the evolution of the analogues of eccentricities e_i, inclinations i_i, argument of pericenters ω_i and motions of the longitude of the ascending nodes Ω_i, the longitude of pericenters π_i given by

$$e_i^2 = \frac{\ni_{\xi_i}^2 + \ni_{\eta_i}^2}{\Lambda_i}, \quad \sin^2 i_i = \frac{\ni_{p_i}^2 + \ni_{q_i}^2}{\Lambda_i},$$
$$\Omega_i = -arctg\frac{\ni_{q_i}}{\ni_{p_i}}, \quad \pi_i = -arctg\frac{\ni_{\eta_i}}{\ni_{\xi_i}}, \quad \omega_i = \pi_i - \Omega_i, \quad i = 1, 2.$$

It should be noted that all of the analytical calculations have been done with the use of the system Wolfram Mathematica (Refs. [7]).

4 Conclusion

In the paper a general problem of three mutually attracting spherical celestial bodies with variable masses changing anisotropically in different rates is considered. A system of eight differential equations of the first order describing the secular perturbations of the orbital elements is obtained in terms of the analogues of the second system of the Poincaré elements in the presence of reactive forces. Approximate analytical solutions of these equations are found by the method of Picard. On the basis of these solutions it is possible to analyze the evolution of the analogues of orbital elements of the bodies that will be done if the next paper.

References

[1] M. Minglibayev, *Dinamika gravitiruyushchikh tel s peremennymi massami i razmerami. Postupatel'noye i postupatel'no-vrashchatel'noye dvizheniye*, LAP LAMBERT Academic Publishing, 229 p. (2012).

[2] I.V. Meshcherskiy, *Raboty po mekhanike tel peremennoy massy*, Moskva-Leningrad, Gostekhizdat, 276 p. (1949).

[3] L.G. Luk'yanov, *Dynamical evolution of stellar orbits in close binary systems with conservative mass transfer*, Astronomy reports, **85**, 8, pp. 755-768 (2008).

[4] M.Dzh. Minglibayev, G.M. Mayemerova, Zh.U. Imanova, *Uravneniya dvizheniya zadachi trekh tel s peremennymi massami pri nalichii reaktivnykh sil*, Vestnik ENU im. L.N. Gumileva, **111**, 2, pp. 19-25 (2016).

[5] A.N. Prokopenya, M.Zh. Minglibayev, G.M. Mayemerova, *Symbolic calculations in studying the problem of three bodies with variable masses*, Programming and Computer Software, **40**, 2, pp. 79-85 (2014).

[6] M.Zh. Minglibayev, G.M. Mayemerova, *Evolution of the orbital-plane orientations in the two-protoplanet three-body problem with variable masses*, Astronomy Reports, **58**, 9, pp. 667-677 (2014).

[7] A.N. Prokopenya, *Resheniye fizicheskikh zadach s ispol'zovaniyem sistemy Mathematica*, Brest, BSTU Publishing, 260 p. (2005).

S2
Computer Algebra in Education

Developing Competences in Higher Mathematics in a CAS Supported Learning Environment

E. Varbanova[1], M. Durcheva[2]

[1] *Technical University of Sofia, Bulgaria, elvar@tu-sofia.bg*
[2] *Technical University of Sofia, Bulgaria, mdurcheva66@gmail.com*

1. Competency-based Objectives as a Challenge to the University Culture

At the Technical University of Sofia the teaching and learning of Higher mathematics aims at the synergy of two modes of learning: traditional mode and technology supported mode. The effect of synergy of their advantages as well as the danger of synergy of their drawbacks need attention. Any combination of these two modes is referred to as blended learning. There exist many different versions of their combination as a result of teachers' creativity in the design and development of learning scenarios. Harmonized and successful scenarios will be further produced by teachers: it takes time and requires experience.

The term 'competence or competency' is widely used in varying ways. The use depends on the context: competence has different emphasis in business processes than in formal education organizations or in theoretical discussion. The term 'key competences' appears in the guidelines of the Bologna Process, the European frame of reference for the reform of higher education ([1, 2]). In Refs. [4] the principal practices and approaches with regard to the development and assessment of individual competencies have been reported. In the light of the current and future impact of this rapidly evolving field on the Competency Frameworks , it is expected mathematics teachers to update the principles and approaches in mathematics education in order to reflect the latest evolutions. Various frameworks have been developed to aid in the development of competencies outlining what graduates should know and be able "to do" as a result of their education [3].

The term 'competency' aims at the identity of the student and his/her deliberate action while dealing with complex tasks and challenges. It has multiple layers and is applied as competence-in-something, including both cognitive and non-cognitive dimensions [1]. Its cognitive meaning designates subject-related and general cognitive abilities up to comprehension and problem-solving, whereas its action-based meaning contains cognitive but also motivational, emotional, social and value-related components. Key competences [2] encompass generative, context-independent abilities and are closely related to action competences.

2. Developing Competences in Higher Education

Competences are part of today's curricula in higher education. They are the objective of a contemporary education: some are explicit learning objectives, others are implicitly contained in studying. The re-orientation of the *curricula towards outcome and competency* makes students autonomous responsible subjects in the teaching-learning-assessment (TLA) process. TLA have to go beyond declarative knowledge and skills and lead to *procedural competences of problem solving*. Both teachers and students face each other in new roles in the TLA process: *the teachers as 'facilitators'* - demanding and encouraging the students, *the students as active partners*. Both sides purposefully work to achieve the educational objectives.

The shift from teaching to learning provides for a frame of orientation and development, that it brings to the fore the freedom of the individual learner that is inherent in the studying process. Competence-based objectives assure more freedom compared to knowledge-based goals. As an ability of handling knowledge, competences can be seen as an open integral of various possible learning contents.

3. A Combined Learning Environment for the Acquisition of Competences in Higher Mathematics

The integrative and additive support with CAS incorporated in blended learning can help lead the students to a connection with subject-specific competences. Lectures, seminars and laboratory classes in Mathematics are to connect key competences with mathematics-related competences through extended learning environments. Depending on the assessment model CAS can often come to the rescue - the student can use the entire potential of CAS during the semester for different purposes of each assessment tasks in both models: continuous assessment and formative assessment with elements of continuous.

In order to be effective, a combined learning environment is to aim at competences beyond knowledge: self-exploring and self-reflecting as well as being opened up for communication and feedback.

As a demonstration of the above mentioned issues the students' work on a set of tasks - guided by teachers, will be presented. One such task suitable for individual task, independent learning or coursework is the following:

Task 1. Determine the values of the real parameter $m \in \mathbf{R}$ for which the equation

$$f(x) = (2-m)x^3 - 3mx^2 - 3mx + 2 - m = 0 \tag{1}$$

has a double root. This type of tasks could bring to the fore the student conscious activity. Learning and assessment activities as well as competences and key competences (such like Life Long Learning) will be discussed.

4. Conclusion

There is "no way back", i.e. no education, progress and development without technology. Digital mathematics exists and digital resistance is not appropriate.

References

[1] D. Chur, *Developing Key Competences In Higher Education*. In Bauder-Begerow, I. Schäfer, S. (Hrsg.) Learning 9/11 - Teaching for Key Competences in Literary and Cultural Studies., Heidelberg: Winter Verlag, 53-74 [PDF-Datei] (2011).

[2] D. Chur, *Kompetenzorientierung im Studium und der Erwerb von Schlusselkompetenzen*. In: Kossek B. Zwiauer C. (Hrsg.): Universität in Zeiten von Bologna. Zur Theorie und Praxis von Lehr- und Lernkulturen. Wien: VR unipress, 289-314 [PDF-Datei] (2012).

[3] K. Ford, *Competency-Based Education; History, Opportunities, and Challenges, UMUC Information and Research Analysis Center for Innovation* In Learning and Student Success (CILSS) (2014) https://www.umuc.edu/innovatelearning/upload/cbe-lit-review-ford.pdf

[4] *TRACE Project (TRAnsparent Competences in Europe)*, Overviiew of European Competency Frameworks, http://www.menon.org/wp-content/uploads/2012/11/9.-TRACE-Overview-of-EU-competency-frameworks1.pdf, (2012)

Improving mathematical competences by using modern technology

Jens Weitendorf[1]

[1] *Norderstedt, Germany JWeitendorf@t-online.de*

Normally when you want to use modern technology in the classroom, you are looking for exercises for those it is easier to solve them using the technology.

In my talk I want to discuss an opportunity to deal with the curriculum on a higher level. This means that you do not have to change the curriculum but you have to change the point of view. The main issue will be the functional aspect of mathematical ideas. For example if you discuss the square function you can start with the universal form of the square function and then the students will be able to find out the influence of the three variables by themselves. Functions are represented by equations, tables or graphs. Using technology it is quite easy to change between those representations.

It will not be possible to discuss the whole curriculum. Therefore I will put my focus on the curriculum for year 7 up to year 9/10 and will give an idea, what is possible using technology. The way through the curriculum will start with the percentage calculation and end with exponential and trigonometric functions. The helpful modern technology will be the ClassPad 400.

To give an impression I will describe some examples. First I want to show how linear equations can be solved by using the ClassPad or any other CAS.

We start with the equation $2x+3=0,5x-2$ (see fig. 1). You put the equation in brackets and put the conversion behind. For students it is helpful to do this because they only have to think about the way of conversation and the calculator will do the calculation. Each part of the equation is the term of a linear function. Therefore you can easily show the corresponding graph. The solution of the equation is the x-value of the point of intersection. The y-value changes. So it is necessary to discuss the connections between changes in algebra and geometry. The following mistake is quite popular:

$$\begin{aligned} 3x+4 &= 7|-3 \\ x+4 &= 4 \end{aligned}$$

The CAS will show the student that his idea will lead to: $3x+1=4$. So the CAS will help to prevent those kinds of mistakes.

The next example will show the connection between a constructed curve and the square function.

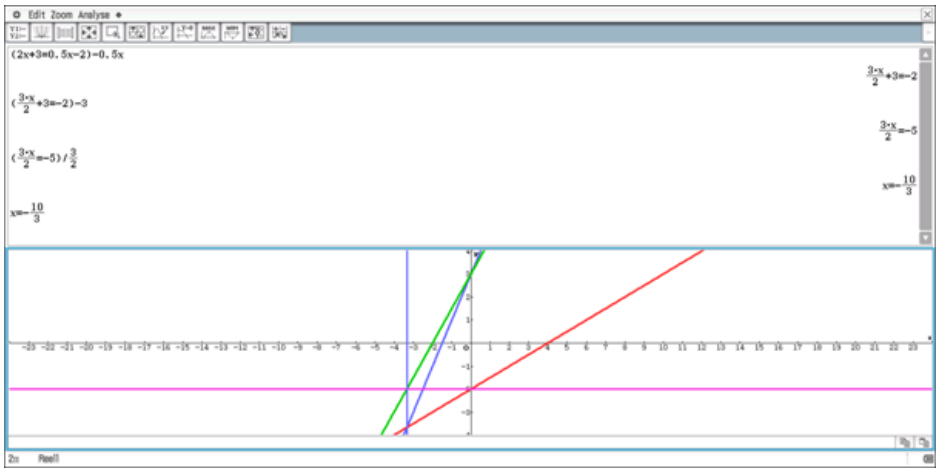


Figure 1: Solving linear equations

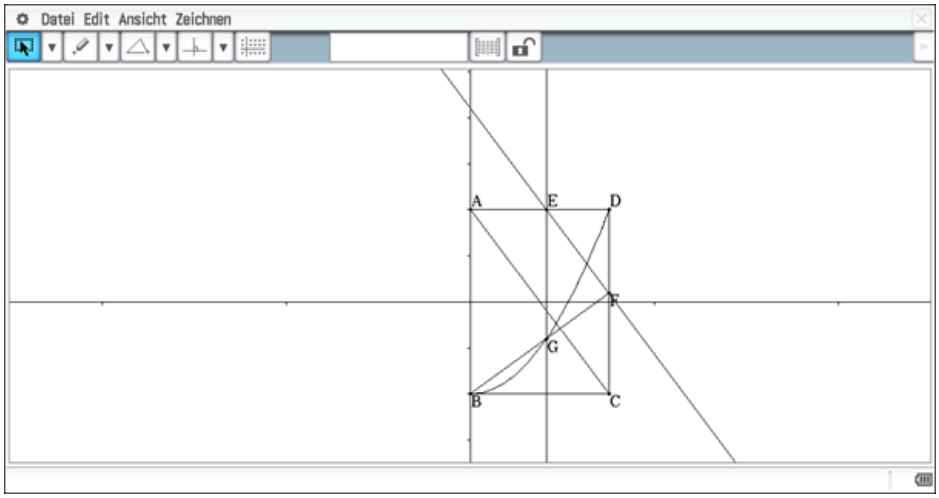
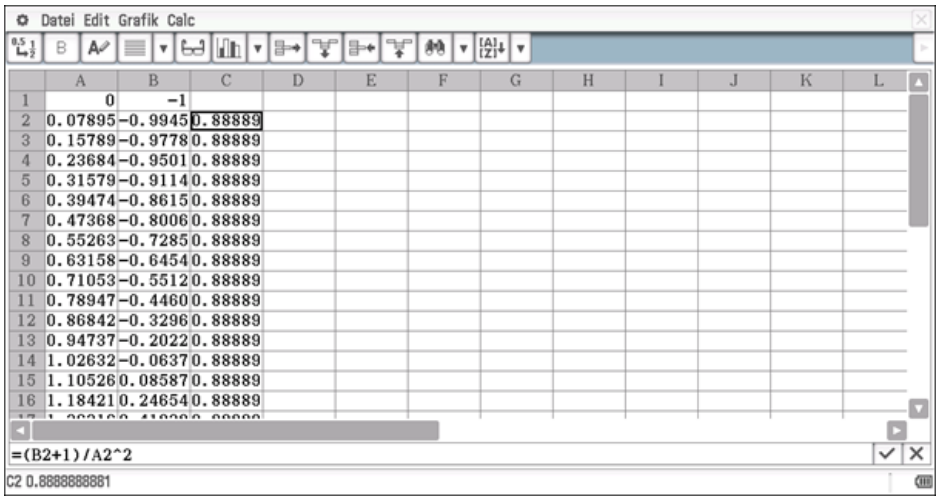


Figure 2: Constructing a parabolic curve



	A	B	C
1	0	−1	
2	0.07895	−0.9945	0.88889
3	0.15789	−0.9778	0.88889
4	0.23684	−0.9501	0.88889
5	0.31579	−0.9114	0.88889
6	0.39474	−0.8615	0.88889
7	0.47368	−0.8006	0.88889
8	0.55263	−0.7285	0.88889
9	0.63158	−0.6454	0.88889
10	0.71053	−0.5512	0.88889
11	0.78947	−0.4460	0.88889
12	0.86842	−0.3296	0.88889
13	0.94737	−0.2022	0.88889
14	1.02632	−0.0637	0.88889
15	1.10526	0.08587	0.88889
16	1.18421	0.24654	0.88889

Figure 3: Analysing the data

The rectangle ABCD is constructed (see fig. 2). The point E is put on the line AD and a parallel to the diagonal AC is drawn. F is the point of intersection and is connected with the point B of the rectangle. The point G is the point of intersection between the line BF and the parallel to the line DC through E. You will get the parabolic curve by animation of the point E. The question is whether it is true that you have got really a parabolic curve. The different coordinates of the point G are saved by the ClassPad. Therefore it is possible to work with them in the spreadsheet (see fig. 3).

This is not a proof of course, but it gives the students an idea of working with data. The proof has to be done afterwards in the classroom. And the question whether a proof is necessary or not must be put up for discussion.

The last example will deal with a problem for older students. We want to get a formula for the curvature of a graph of a function. Therefore you can start with a special function and a special point.

We discuss the graph of the square function $f(x) = x^2$ and the point $(0/0)$. A circle is constructed with centre A, which is variable on the y-axis, and the point $B(0/0)$. The students can find out that the circle and the parabolic curve have one or three common points. The crossing-point is of special interest. This leads to the definition of what is meant by the curvature of a graph.

In the situation of the crossing-point the following equations must be true:
Square function: $f(x) = x^2$
Part of the circle: $c(x) = r - \sqrt{r^2 - x^2}$

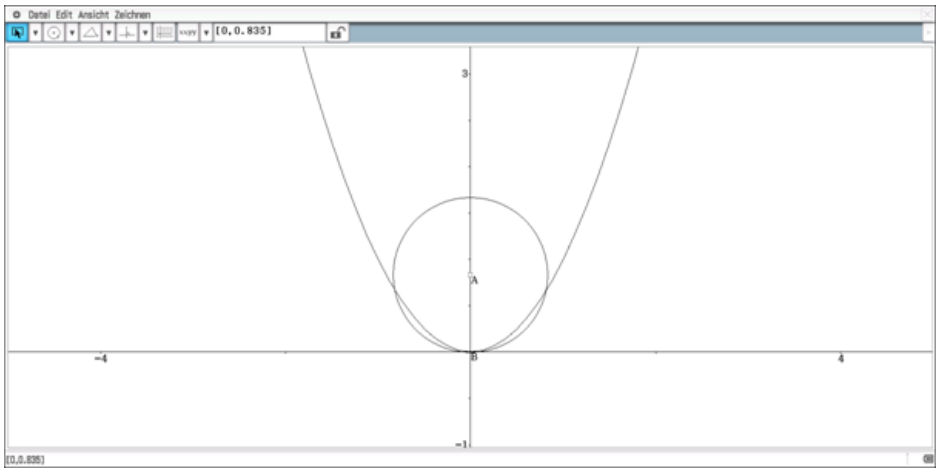


Figure 4: Parabolic curve and responding circle

The three equations:

$$f(0) = c(0) \qquad f'(0) = c'(0) \qquad f''(0) = c''(0)$$

You can generalize those three equations to any function and any point and a CAS like the ClassPad will be able to create the formula.

Applications of CAS in the Teaching and Learning of Discrete Mathematics

M. Durcheva[1], E. Varbanova[2]

[1] *Technical University of Sofia, Bulgaria, mdurcheva66@gmail.com*
[2] *Technical University of Sofia, Bulgaria, elvar@tu-sofia.bg*

Discrete Mathematics is a compulsory course in the curriculum of the Bachelor Degree Program at the Faculty of Applied Mathematics and Informatics of the Technical University of Sofia (TUS). Discrete structures are taught also to engineering students at TUS.

As it is reported in Refs. [1, 2]), the following competences of the above mentioned students are to be developed: thinking mathematically; reasoning mathematically; posing and solving mathematical problems; modeling mathematically; representing mathematical entities; handling mathematical symbols and formalism; communicating in, with, and about mathematics; making use of aids and tools. How could applications of CAS contribute to this educational goal? It is often necessary to manipulate big data in discrete mathematics, mainly for the purpose of combinatorics, recurrence relations, formal logic, Boolean algebra. For that reason formulas have very limited range of use. The application of CAS can help expand these limits significantly. The most important thing is how learning can be enhanced by the use of CAS.

Concurrent implementation of pedagogy and technology requires consideration of current practices, including the activities and expectations of learners and teachers. Technology allows students to work with more complex and realistic models since work within the model is supported by technology and even the setup of models can be facilitated by technology. In engineering programs, models are often only partially visible, so students need to learn to work with technology where the underlying model is not known to them. This requires knowledge about strategies for checking one's understanding of the workings of the program and also for checking the results.

In this paper our experience in application of CAS MAPLE for modeling discrete structures is represented. Some procedures for calculating combinations with repetition and variations with repetition in case of arbitrary restrictions on appearance of elements are considered. The result is the list of the allowed number of appearances of the element in the polynomial involved in the generated function (see Refs. [4]). Some conclusions are visualized. Solving recurrence equations with MAPLE (Refs. [3])) is also discussed.

References

[1] *A Framework for Mathematics Curricula in Engineering Education*, A Report of the Mathematics Working Group, European Society for Engineering Education (SEFI), Brussels, 2013, Principal Editor: Burkhard Alpers.

[2] M. Niss and T. Hojgaard, *Competencies and Mathematical Learning Ideas and inspiration for the development of mathematics teaching and learning in Denmark*, IMFUFA tekst nr. 485/ 2011.

[3] K. Rosen, *Discrete Mathematics and Its Applications*, Seventh ed., 2016, McGraw-Hill Global Education Holdings, LLC.

[4] H. Wilf, *Generatingfunctionology*, Academic Press, Inc., New York, 1994.

A Transparent Rule Based CAS to support Formalization of Knowledge

R. Oldenburg[1]

[1] *University of Augsburg, Germany, reinhard.oldenburg@math.uni-augsburg.de*

Algebra is an important and highly complicated subject of schools mathematics that can be structured according to various dimensions of analysis, e.g. it comprises different kinds of activities [2] and structures that obey different linguistic systems [3]. This paper is written in the spirit of that last reference and takes the linguistic view of mathematics to include syntactical, semantical and pragmatic aspects of the algebraic language. Syntactical aspects of algebra can easily be handled by computer algebra systems (CAS). However, there is evidence (e.g. [4] but many others) that students have great difficulty to understand what a CAS does and how its output is to be interpreted. Thus, we conducted a small developmental research project that aimed at producing a prototype of a CAS that is as transparent to students as possible. We hope that students can understand how this system works completely and furthermore, it is hoped that they can use it to formalise their mathematical knowledge by making the system more powerful by giving additional rules. So the ideas is to extend Papert's idea of the computer as a trainee to the realm of computer algebra.

The system developed is called SCAS (simple syntactical CAS, doubling the S in the acronym was avoided for obvious reasons) aims to support the learning of syntactical aspects of algebra as well to provide a simple mental model of what a computer algebra system (CAS) is and how it works. The basic use of SCAS is similar to other CAS: You enter an expression and the system answers with an output. E.g. if you enter `2*x+y+x+3` then the system answers `3*x+y+3`.

SCAS is a rule based term rewriting system [1]. Of course, modern CAS are not (completely) rule based as many operations have much more efficient algorithmic solutions than those possible by term rewriting. Nevertheless, we believe that this gives a good mental model of the syntactic way a CAS treats mathematical expressions.

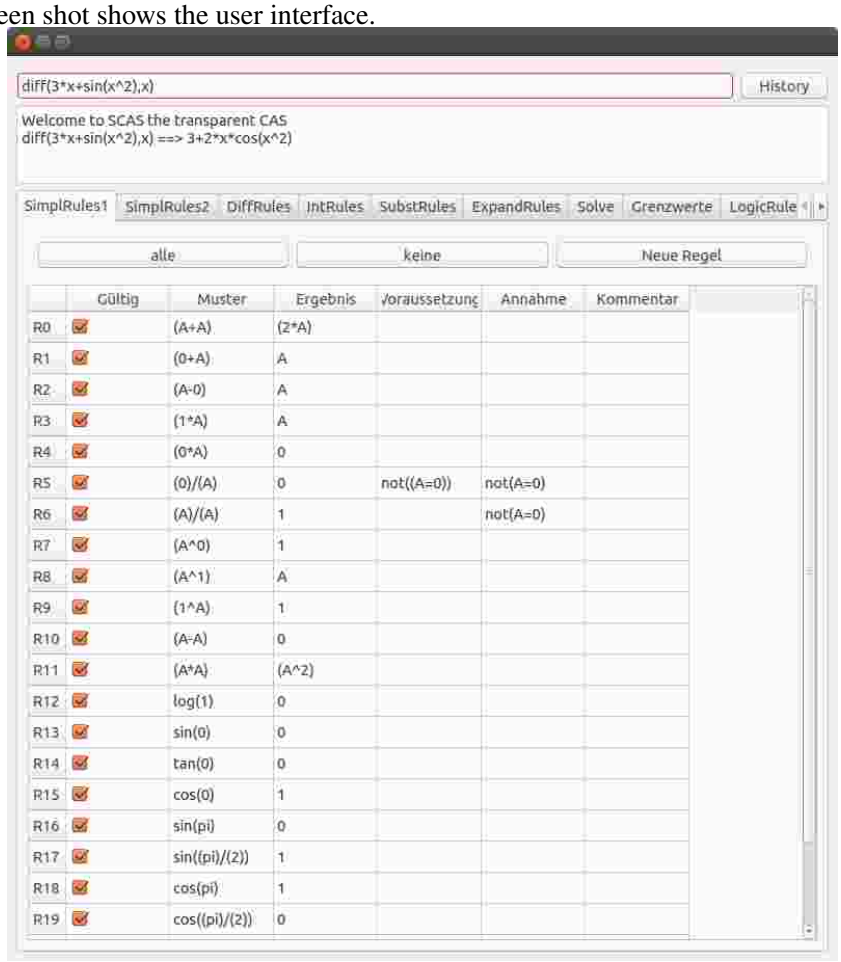
The following simple rules govern the behaviour of the system:

- All expressions are represented by binary trees (e.g. `a+b+c` is interpreted as `a+(b+c)`)
- There is a list of rewrite rules. A rule consists of a pattern, possibly a condition, and a replacement. A handy notation is *pattern*→*replacement*. The

system goes through this list of rules and with each rule it checks if it can be applied to any sub-expression of the current expression. If so it checks if the condition of the rule is satisfied, and if this is the case the expression is replaced.

- This process is repeated until no applicable rule is in the rule list. The final expression is send to the output.

Students can turn on or of indivudal rules like `A-A→ 0` or rule groups (like that for expanding). Moreover, they can enter new rules. The idea is to give them the opportunity to formalize their knowlede e.g. about derivatives. The following screen shot shows the user interface.



The talk will discuss the design ideas and show the system as well as further didactical questions.

References

[1] F. Baader, T. Nipkow, *Term Rewriting and All That*, Cambridge UP, Cambridge (1999).

[2] C. Kieran, *The core of algebra: reflections on its main activities.*, in K. Stacey et al. (eds.), The future of the teaching and learning of algebra. Kluwer Academic Publishers, Dordrecht (ISBN 1-4020-8130-8), pp. 21-33 (2004).

[3] J. Hodgen, D. Kuechemann, R. Oldenburg, *Syntactic and Semantic Items in Algebra Tests - A conceptual and empirical view*, CERME 2013.

[4] R. Oldenburg, B. Weygandt, *Einsatzmöglichkeiten und Grenzen von Computeralgebrasystemen zur Förderung der Konzeptentwicklung*, in A. Hoppenbrock et al. (eds.) Lehren und Lernen von Mathematik in der Studieneingangsphase. Springer, Berlin (2015).

The GUI CATO – how natural usage of CAS with CATO modified the mathematical lectures and the interface itself

H.-D. Janetzko[1],

[1] *Mathematikbüro Janetzko, Lübeck, Germany, formerly HTWG Konstanz, janetzko@mathematikbuero.de*

CATO is a German user interface for different computer algebra systems written in Java. The author develops CATO as a response to the significant difficulties faced by those engineers and students who only sporadically use computer algebra systems. The usage of CAS in mathematical lectures should be an integral part of mathematical instructions. However, difficulties arise for students when lecturers employ CAS only once or twice a week in their lecture. In the author's experience, the usage of CAS is often perceived by the students as an unnecessary further burden. Using CATO, the general user interface for CAS, there are no obstacles for the students, also for the weaker. The author describes some experiences using CATO linked with Mathematica, Maxima or the mathematical toolbox of MATLAB.

Previous approaches and considerations

There are many reasons for the usage of a computer algebra system in teaching mathematics (see, for example [1] or general [3]. But the usage of CAS in a mathematical lecture can distract from the mathematics itself, for example [4].

The demand for better designs of user interfaces for computer algebra systems is almost as old as the systems themselves. Kajler has described and developed his ideas for a perfect user interface in various works and elaborated these in further works (for example [5]). Kajler has postulated that well-designed computer algebra interfaces should afford intuitive access. As such, they should enable the entry of commands with more than one parameter by a two-dimensional layout. This prevents syntactic and structural errors. In addition, all templates and masks should follow the convention of operating from left to right. Intuitive interfaces should also apply conventional mathematical notations, and decouple the surface from the computer algebra systems. The interface should be serviced independently, and regularly developed and updated. Ideally, it should understand a range of computer algebra systems.

The author himself has used various computer algebra systems in his mathematics courses at the University of Applied Sciences (HTWG) in Konstanz, beginning with Maple, followed by Mathematica, and finally Maxima. His experiences of students' occasional usage of CAS in mathematics courses are complex; he has

observed that the experience is not necessarily positive for all students. Only some students are fascinated by the usage of a CAS, and independently explore its potential. A larger proportion of students accepts CAS, but learns only those commands it considers necessary to prepare for upcoming examinations. Enough students treat the learning of the vocabulary, syntax and grammar required for the usage of CAS as an unwelcome burden, and consequently gives up on mathematics. The majority, therefore, never see the opportunities provided by computer algebra as a mathematical aid, [2].

The author wants to balance the difficulties of learning to use a computer algebra system with the benefits of using it. He has developed an interface to use a computer algebra system without distraction from mathematics, called the Computer Algebra Taschenrechner (Calculator) Oberfläche (surface) or CATO for short. In his intention, students should be able to successfully use CATO, even if their knowledge of mathematics was limited.

The usage of CATO

The author uses CATO in the courses Mathematics One and Two in the Bachelor of Electrical Information Technology degree program. The University of Applied Sciences does not offer a general "Introduction to Computer Algebra" course. Consequently, the author introduces students to the use of CATO in his first lecture, after describing what a computer algebra system is, and why it makes sense to use it. His students use CATO in the computer lab during the first week of lectures to calculate three examples: differentiating, solving an equation, and plot a function. Once they have done this, they grasp the concept and the structure of CATO, and are able to use CATO without explicitly learning it (for example Janetzko 2015). The students (including the weaker ones) are confident that CAS with CATO is no further obstacle to pass the exam. They believe the structures of CATO create no additional difficulties to use CAS.

Launching CATO, the student sees a surface like a graphical pocket calculator with an input and an output window on the left hand. Below them there are several menus. All commands can be selected via packages and menus. The commands are grouped in packages or sub-packages. The packages group related commands together: The menu with all packages is located at the bottom left. If one package is selected, the commands of the selected package will be loaded in the menu right next to it. For example, if the student selects the package "statistics" on the highest hierarchy level, several statistic related subpackages will be shown in the menu right next to the first one. After selecting a subpackage like "normal distribution" or "descriptive statistics", the commands of this one will be loaded in the third menu at the bottom right next to the second menu.

After selecting a command with more than one parameter, the student gets a new input window with one row for every parameter. Each multi-parameter command has its own input window.

For example, the window of the command “n-th derivative” has three input lines: “function”, “variable”, “n =”. The order of the input line is always independent of the used CAS. CATO itself sorts the input according to the respective CAS. (Additional a short description of the command is a part of this extra window.)

Other concepts realized in CATO

In writing CATO, the author has developed, adopted, and implemented many ideas and concepts for ease-of-use. Some ideas can be found in the papers of Kajler. As the author’s primary aim was to allow casual use of computer algebra in his lectures, he has also integrated changes based upon his teaching experience with Maple, Mathematica, and Maxima. Additional modifications have been the result of student feedback.

When the author developed the basic concepts of CATO, he envisioned some commands being contained in more than one package. For example, the command “definition of a vector” is contained in the package “definitions” and in the package “linear algebra”. Some years ago, CATO was enabled to collect the last 20, the last 50, or the last 100 commands residing in a new package. (There was no modification to the internal structures of CATO needed, because of the possibility of one command being member in more the one package.) The author believed it would be a simplification to repeat the same command. But the students meant it was too complicated. So the author extended CATO with the menu and package “chronicle”, it collects all command during a session. The menu “chronicle” is a part of CATO since the change to version 1.2.

Later, the students wanted to save, export and later to import (with a new name) the package “chronicle” at the exam. Their desire was to win some seconds at the exam having a list of all previously used commands.

Like a CAS, CATO has a log containing all command executions and corresponding results. In some cases, students wanted to have more extensive descriptions of the commands in the detailed input window and the log. For commands with more than one parameter, the description in the log and in the input window is usually more extensive than its name in the package. In contrast to normal CAS, in CATO there is a difference in the usage – selection – and the application – input of the parameters – of a command. The author could satisfy all requests for better or more extensive descriptions without modifying the internal structures of CATO and furthermore without modifying the command in the package menus.

Modification in the lessons

The exam in the computer lab consists of two parts: Part one is without any aid. The students receive it at first and when one of them believe, he has solved all tasks, he submits this part. Part two is with aid (naturally with documents), the student can and should use CATO with one CAS at the PC. Of course, there is no connection to the Internet.

Using CATO, teaching has been modified in the desired way. The author can use CAS for more and more illustrative examples, often examples helping to answer some comprehension questions. Furthermore, very long calculations can be shorted to the crucial parts. Priorities are newly settled as shown in the following old exercise:

We consider a bottling plant for milk. The milk in the bottles can described by normal distribution with $\mu = 1001$ *ml and* $\sigma = 1.3$ *ml. Describe the probability to get a bottle with less than* 998 *ml!*

Without CAS you need the quantil of the N(0,1) distribution from a table and the transformation rule of Gauß. But applying CAS the solution is only one (correct) command. Consequently, we need a new exercise:

We can describe the bottling plant for milk in the following way: 5 % of the bottles content less than 997.5 *ml and 2.8 % content more than* 1002.3 *ml. Determine* μ *and* σ*!*

To solve this new kind of exercises, students need a deeper understanding of quantiles and can solve more realistic exercises.

Some changes in students' behaviour

After the eighth to tenth week of lecture, most students explored themselves independently the possibilities of CATO connected with a CAS. This never occurred previously by using a CAS without CATO. The author was able to note the fact; the students questioned the command set of CATO or the cryptic results of the CAS.

The author has of course always questioned in his lectures the potential and the limits of CA by appropriate examples. Only since using CATO there were reactions of students.

Sometimes there are moments in which the teacher must presuppose something and some students have knowledge gaps. The reaction of these students was: "CATO schafft es schon!" ("CATO makes it!"). They are apparently confident that such issues would be assessed only in the exam part with aids and they could bridge their knowledge gaps by CATO commands.

By allowing CATO with a CAS in the exam part with aids, students were able to succeed the exam in Mathematics II despite of significant gaps in Mathematics

I. Whether this is in general useful, you have to consider yourself in dependence of the lecture goals.

Conclusions

In the author's experience, it makes sense to teach mathematics integrating occasional usage of computer algebra systems. The author can only reflect his own experience and describe similar experiences of other teachers, who also used CATO in connection with a CAS. There were no evaluations on student achievement using CATO and a CAS compared with other students for various reasons. The author was the only teacher in this field, who allowed CAS as an aid. The author was an external lecturer. Therefore, there was possibility for parallel lectures, one with CATO and CAS, even without CATO and CAs. Additionally, it would be inappropriate to compare with the lectures before CATO existed, since the usage of CAS highly increased and the content of the lecture changed accordingly. There remains only the usual lecture evaluations in comparison to evaluations of lectures organized by other faculty members, but obviously there are too many other influencing factors.

Currently there are approximately 550 commands for Maxima, 550 commands for Mathematica (version 4.0 or higher), 450 commands for the Mathematical toolbox of MATLAB, 300 commands for Maple (version 9.5 or higher), 350 commands for MuPAD 3, 250 commands for Yacas and 150 commands for MATLAB. In addition, there are more than 50 CATO internal commands. Currently, the German CATO is translated to English and French. Free trial versions of CATO can be downloaded from the author's website at any time, http://www.computeralgebra.biz (also some links or references to articles about CATO).

References

[1] B. Barzel, *Establishing conditions for Computeralgebra as an additional value in mathematics teaching*, in *The 11th International Conference on Technology in Mathematics*, Conference Proceedings, University of Bari, pp. 71- 76 (2013).

[2] H. P. Hornæs and O. Røyrvik *Aptitude, Gender, and Computer Algebra Systems*, Journal of Engineering Education, Volume 89, Issue 3, pp. 323-330 (2000)

[3] N. Kajler, *Computer-human interaction in symbolic computation*, Springer (1998).

[4] J. Lagrange, *Techniques and Concepts in pre-calculus Using CAS: A Two Year Classroom Experiment with the TI-92*, in *International Journal of Computer Algebra in Mathematical Education*, vol 6, no 2, pp 143-165, (1999).

[5] K. Stacey, K. H. Chick and M. Kendal, M. *The Future of the Teaching and Learning of Algebra: The 12th ICMI Study*, Springer, (2004).

Collaborative Use of KeTCindy and Free CASs for Making Materials

Setsuo Takato[1], Alasdair McAndrew[2], Masataka Kaneko[3]

[1] *Toho University, Japan, takato@phar.toho-u.ac.jp*
[2] *Victoria University, Australia, Alasdair.McAndrew@vu.edu.au*
[3] *Toho University, Japan, masataka.kaneko@phar.toho-u.ac.jp*

1 Introduction

Many mathematics teachers at collegiate level use LaTeX to write materials for distribution to their classes. As is well known, LaTeX can typeset complex mathematical formulas. On the other hand, it has poor ability to create figures. One possibility might be to use a third-party package, such as TiKZ. However, TiKZ coding is complicated and is not easy to read even for the following simple figure.

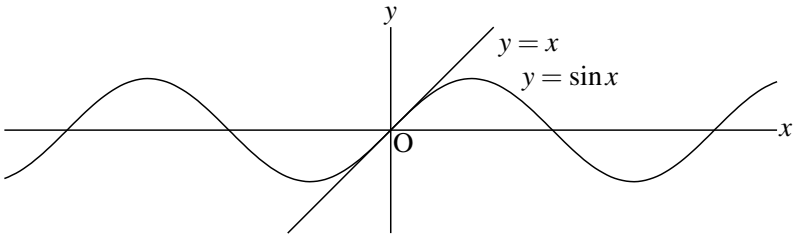


Figure 1 A simple example

TiKZ can in fact produce figures of great complexity, but its power comes at the cost of a steep learning curve. In order to provide a system for easy creation of publication quality figures, the first author has developed KeTpic, the first version of which was released in 2006. KeTpic is a macro package of mathematical software such as Maple, Mathematica, Scilab and R. The recent version uses Scilab mainly and R secondarily.

The flow of generating and inserting graphs with KeTpic is as follows.

1. KeTpic and Scilab commands are listed in a Scilab editor and executed by Scilab.
2. Scilab generates a LaTeX file composed of codes for drawing figures.
3. That file can be inserted into a LaTeX document with `\input` command.
4. The document can be compiled to produce a pdf file.

Scripts for Figure 1 are as follows.

```
Setwindow([-7.5,7.5],[-2,2]);
Setax(7,"se");
gr1=Plotdata("sin(x)","x");
gr2=Plotdata("x","x","Num=1");
Openfile("figsin");
  Drwline(gr1,gr2);
  Expr([2.5,1],"e","y=\sin x",[2,1.5],"e","y=x");
Closefile('1');
```

Scripts of KETpic are far more readable than those of TiKZ, and the simplicity of the scripts provides for a simple method of inserting figures into LaTeX.

However, it is cumbersome to write all scripts in the Scilab editor first. In particular, mathematics teachers who are not used to mathematical software may find KETpic hard to use. One of the long-standing plans for KETpic has been to write a graphical user interface(GUI) for it.

2 Development of KETCindy

Cinderella[1] is a dynamic geometry software(DGS), and was developed by Gebert and Kortenkamp. The first author had been searching for the possibility of collaborating KETpic and Cinderella with Kortenkamp, and the first version of KETCindy was released in September, 2014. Cinderella works as GUI of KETCindy. It has two screens for the display of figures and for the editor of CindyScript, which is a programming language of Cinderella. To draw a figure,

1. Put geometric components such as points and segments on the display.
2. Describe scripts for drawing a figure and generating of LaTeX graphic codes.
3. Press two buttons on the display to execute batch processing of Scilab, LaTeX compiling and viewing PDF sequentially.

Then you can get the objective figure of LaTeX.

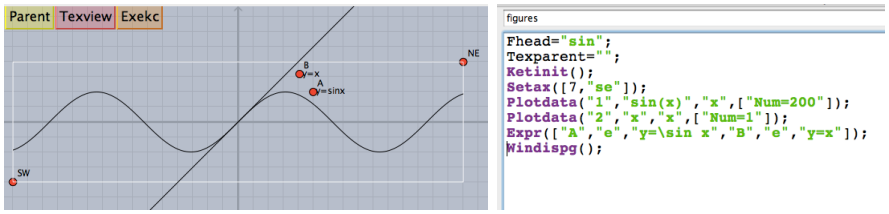


Figure 2 Screens of Cinderella

So far, KETCindy can generate various types of figures or tables as follows.

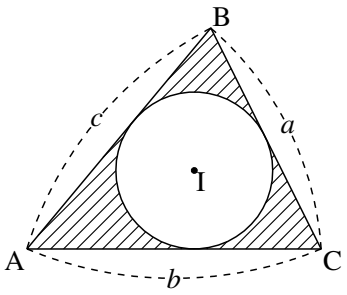


Figure 3 Geometric Figure

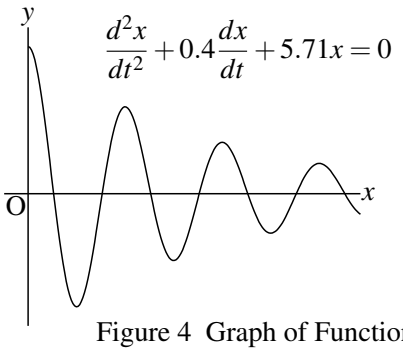


Figure 4 Graph of Function

x	0	$\cdots$	e	$\cdots$	$e\sqrt{e}$	$\cdots$
y'		+	0	−	−	−
y''		−	−	−	0	+
y			$\frac{10}{e}$		$\frac{15}{e\sqrt{e}}$	

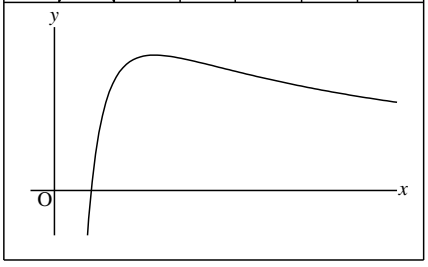
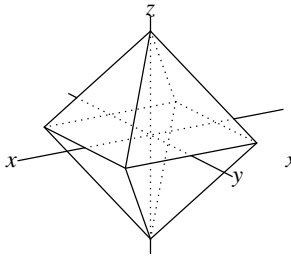


Figure 5 Table

Figure 6 Bézier Curve

3D figures such like the followings can be produced by KETCindy.

```
Xyzax3data("","x=[-5,5]","y=[-5,5]","z=[-4,4]");
polydt=Readobj("r02.obj",["size=-3.5"]);
VertexEdgeFace("1",polydt,["Pt=fix","Edg=nogeo"]);
Nohiddenbyfaces("1","phf3d1",[],["do"]);
```



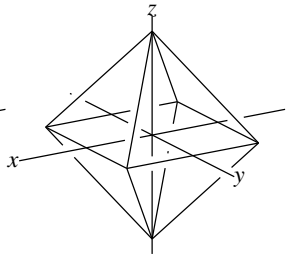


Figure 7 Polyhedron

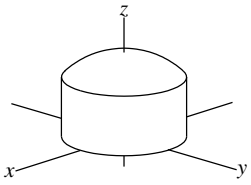


Figure 8 Surface

KETCindy is downloadable from `http://ketpic.com/?lang=english`.

3 Calling CASs from KETCindy

Recently, we implemented functionality to call CASs such as Maxima and FriCAS. In this section, we introduce the functionality and show some application in mathematics education.

The flow and chart are as follows.

1. To generate the shell file to call a CAS
2. To execute the file
3. To return the result as text
4. To use the result in KETCindy
5. To produce the PDF file

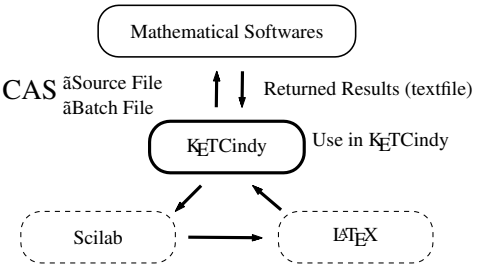


Figure 9 Chart of KETCindy

We give an example to find points of contact of two curves.

```
Mxfun("1","solve",["[y=x^2, x^2+(y-1)^2=3/4]","[x,y]"],[""]);
P=parse(mx1)_1; Q=parse(mx1)_2;
Plotdata("1","x^2","x");
Circledata("1",[A,P]);
Listplot("1",[P,A,Q]);
Letter([A,"ne","A",P,"sw","P",Q,"se","Q"]);
```

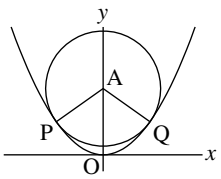


Figure 10

The use of a computer algebra system is required for use with KETCindy and in keeping with the open-source nature of the project, we choose an open-source system. Of the many available, we are most interested in Maxima and FriCAS, being open-source version of once commercial software: Macysma and IBM Axiom respectively. Maxima is written in Lisp and C, and can run on any system which supports those languages. In particular, Maxima can run under MS Windows, Linux, and MacOS. There are even versions of portable systems such as Android. Maxima, formally, is a "term-rewriting" system, where by a system of rules (which the user can add to or change) a term can be rewritten in another form. Thus there are formal rules for symbolic differentiation, for applying integral transforms, for linear algebra, and so on.

FriCAS is a fork of the CAS Axiom, which was released as open-source by IBM when it became clear it was losing its market share. In comparison to all other CAS's today, FriCAS is *strongly typed*: each expression, variable or other object belongs to a particular type, or nest of types. The use of types allows for overwriting of operations, so that, for example, the outcome of a multiplication '`x * y`' will depend on the types of `x` and `y`. The nesting of types means that you can

define, for example, square matrices of polynomials over a finite field, and having defined that type you automatically have operations available: an inverse of such a matrix, for example, will produce an output object of the same type. The use of types is confusing for the beginner, but in fact provides immense power for the exploration of mathematical systems. In that sense FriCAS probably has greater depth than any other system, although it loses out on breadth.

For systems which are to be used as black boxes: question in, answer out, Maxima may be preferred because of its breadth. But for a system where mathematical precision and rigour are required, FriCAS is the best choice. FriCAS however works best under Linux, so its use in a Windows system requires either some Unix subsystem (such as Cygwin) or the use of a docker container.

Here we give an example of use of Maxima and FriCAS with KETCindy.

```
fun="((1-cos(t))/(1/2-cos(t)))^(1/2)";
Mxfun("1","integrate",[fun,"t"]); //by Maxima (inadequate)
Frifun("2","integrate",[fun,"t"]); // by Fricas
Mxtex("2",fri2);  // Maxima can generate LaTeX form
```

The result by Fricas is $\displaystyle\int \sqrt{\frac{1-\cos t}{\frac{1}{2}-\cos t}}\,dt = -\arctan\left(\frac{(4\cos t+1)\sqrt{\frac{2\cos t-2}{2\cos t-1}}}{4\sin t}\right)$.

Note that FriCAS implements a nearly complete version of the Risch algorithm for symbolic integration; thus its integration routines are amongst the strongest of any current CAS.

4 Conclusion and Future Work

Printed materials are often used in mathematics classes at collegiate level, and high quality figures are indispensable in such materials. KETCindy makes it easy to produce and insert them. The samples in this paper show that the symbolic computation capability of a CAS can enhance the graphics capability of the KETCindy system. CASs are also useful to produce examples and problems embedded into materials, for example, when we put matrices for Gaussian elimination. Other possibilities of their collaborative use in education should be pursued.

Acknowledgment
This work was supported by JSPS KAKENHI Grant Numbers 25350370, 15K01037, 15K00944.

References

[1] Cinderella, http://www.cinderella.de/tiki-index.php

Visualization of simplex method with Mathematica

Włodzimierz Wojas[1], Jan Krupa[2]

[1] *Warsaw University of Life Sciences (SGGW), Poland,* wlodzimierz_wojas@sggw.pl
[2] *Warsaw University of Life Sciences (SGGW), Poland,* jan_krupa@sggw.pl

Simplex algorithm is taught at universities in framework of different academic courses, for example Linear Programming, Mathematical Programming or Operation Research. One aspect of the teaching of this algorithm is to present a geometric interpretation of simplex steps. Some attempts to visualization simplex method using CAS were taken in papers [1, 4, 5]. In this article, the authors propose some new approach to this subject through the use of expanded Simplex Tableau. This Tableau, for each of simplex step contains: current simplex table for this step, graph of feasible region for standard form of LP problem with current vertex of simplex path, current level set of objective function corresponding to this step (hyperplanes : lines in 2D, planes in 3D), axis with current value of objective function for this step. The presentation was prepared using Mathematica. We present examples for 2D and 3D feasible regions. One of them is presented below.

Example.
Let us visualize simplex steps for the following LP problem in standard form (in $\mathbb{R}^2$):

$$\begin{aligned}
\text{Maximize} \quad & z = 3x_1 + 2x_2 \\
\text{Subject to} \quad & x_1 - 3x_2 \leq 2 \\
& x_1 - x_2 \leq 4 \\
& 5x_1 - x_2 \leq 36 \\
& -4x_1 + \frac{5}{2}x_2 \leq 5 \\
& -x_1 + 4x_2 \leq 16 \\
& x_2 \leq 9 \\
& x_i \geq 0 \text{ for } i = 1, 2.
\end{aligned}$$

Corresponding to it canonical form is:

$$
\begin{array}{lrcl}
\text{Maximize} & z = 3x_1 + 2x_2 & & \\
\text{Subject to} & x_1 - 3x_2 + x_3 & = & 2 \\
& x_1 - x_2 + x_4 & = & 4 \\
& 5x_1 - x_2 + x_5 & = & 36 \\
& -4x_1 + \frac{5}{2}x_2 + x_6 & = & 5 \\
& -x_1 + 4x_2 + x_7 & = & 16 \\
& x_2 + x_8 & = & 9 \\
& x_i \geq 0 \text{ for } i = 1,2,\ldots,8 & &
\end{array}
$$

Feasible region for this LP problem (in standard form) is presented in each Figure 1–5. It is convex polyhedral set with vertices at: $v_1 = (0,0), v_2 = (2,0), v_3 = (5,1), v_4 = (8,4), v_5 = (9,9), v_6 = (6.5,9), v_7 = (2.5,6), v_8 = (0,2)$. In each Figure 1–5 we present expanded Simplex Tableau for subsequent vertices of simplex path.

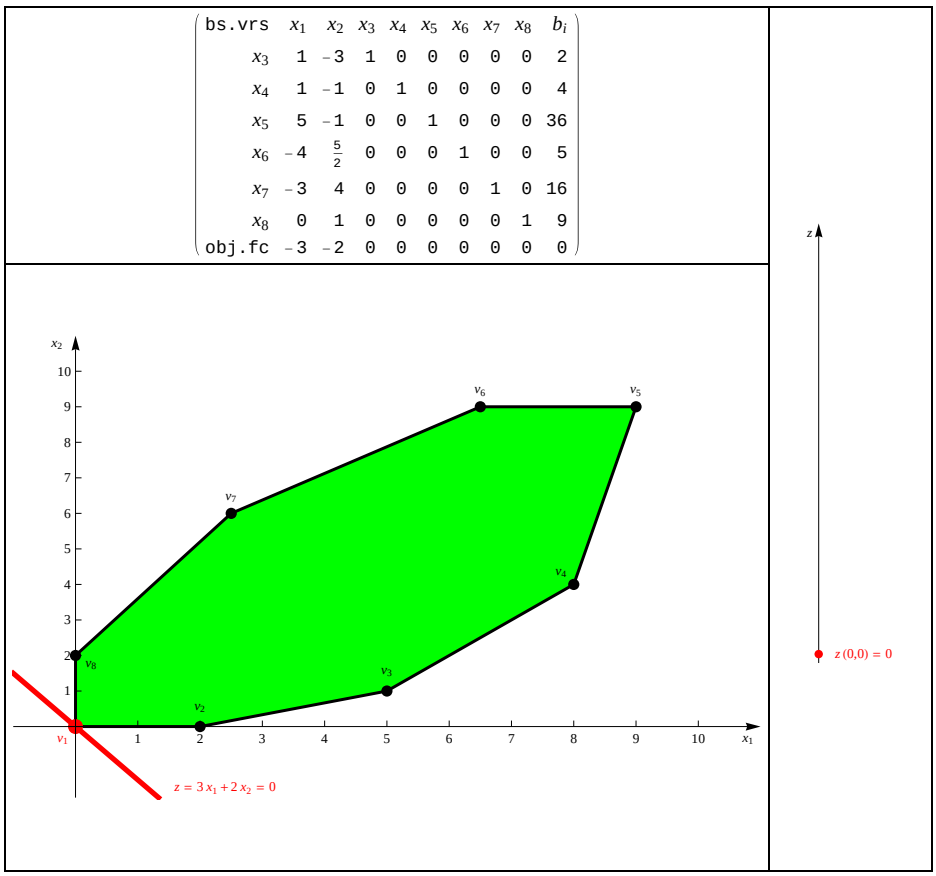


Figure 1: First expanded Simplex Tableau.

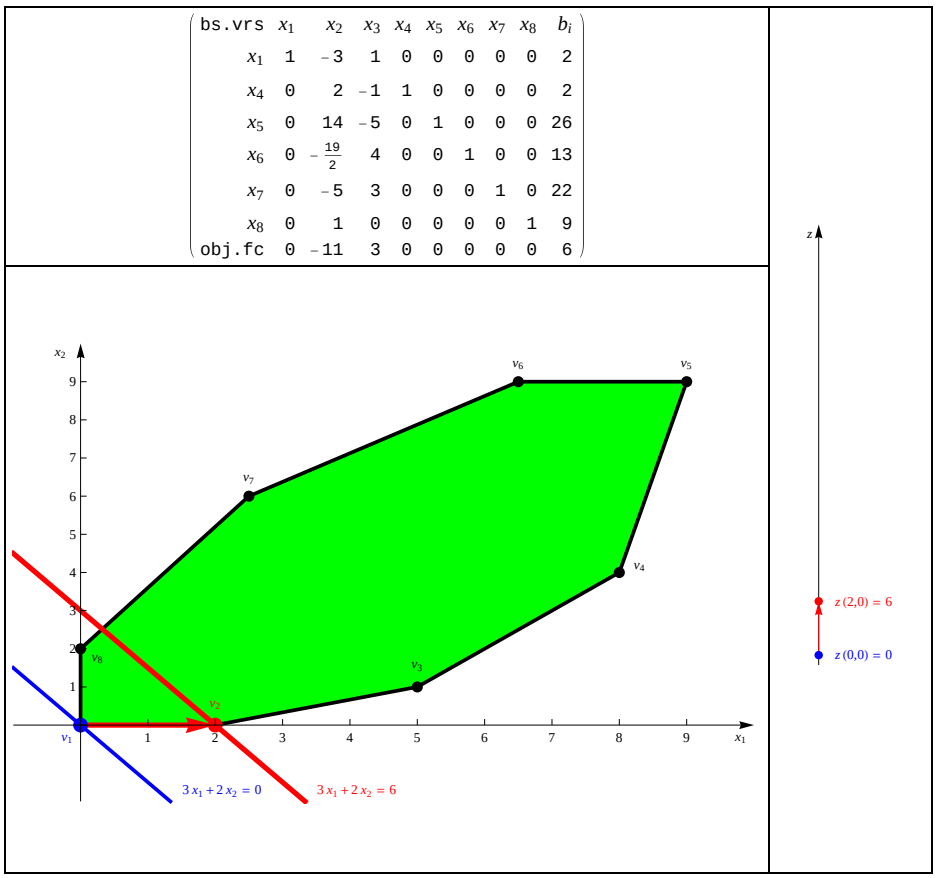


Figure 2: Second expanded Simplex Tableau.

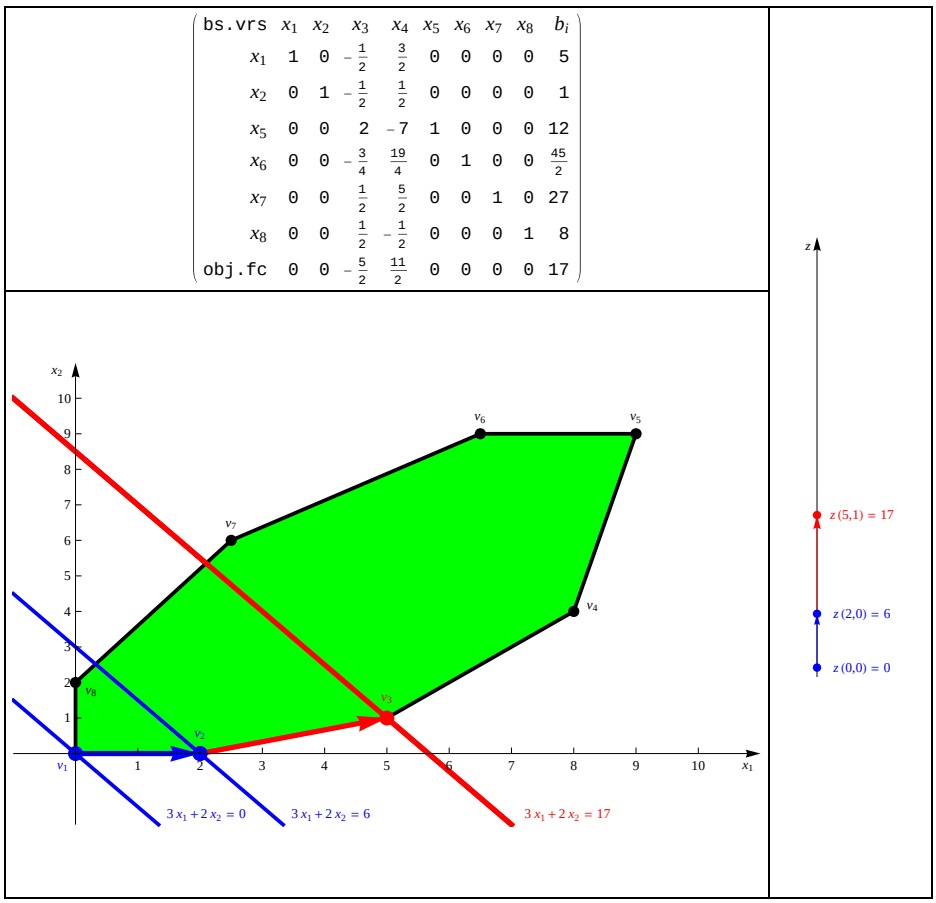


Figure 3: Third expanded Simplex Tableau.

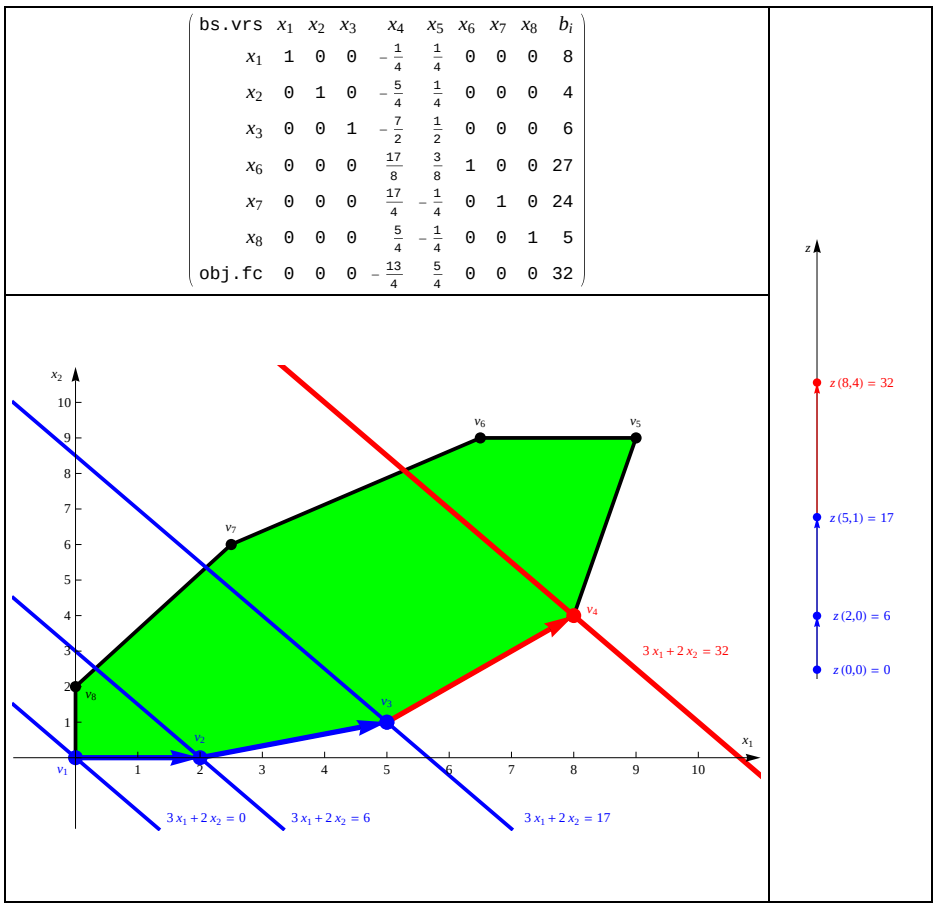


Figure 4: Forth expanded Simplex Tableau.

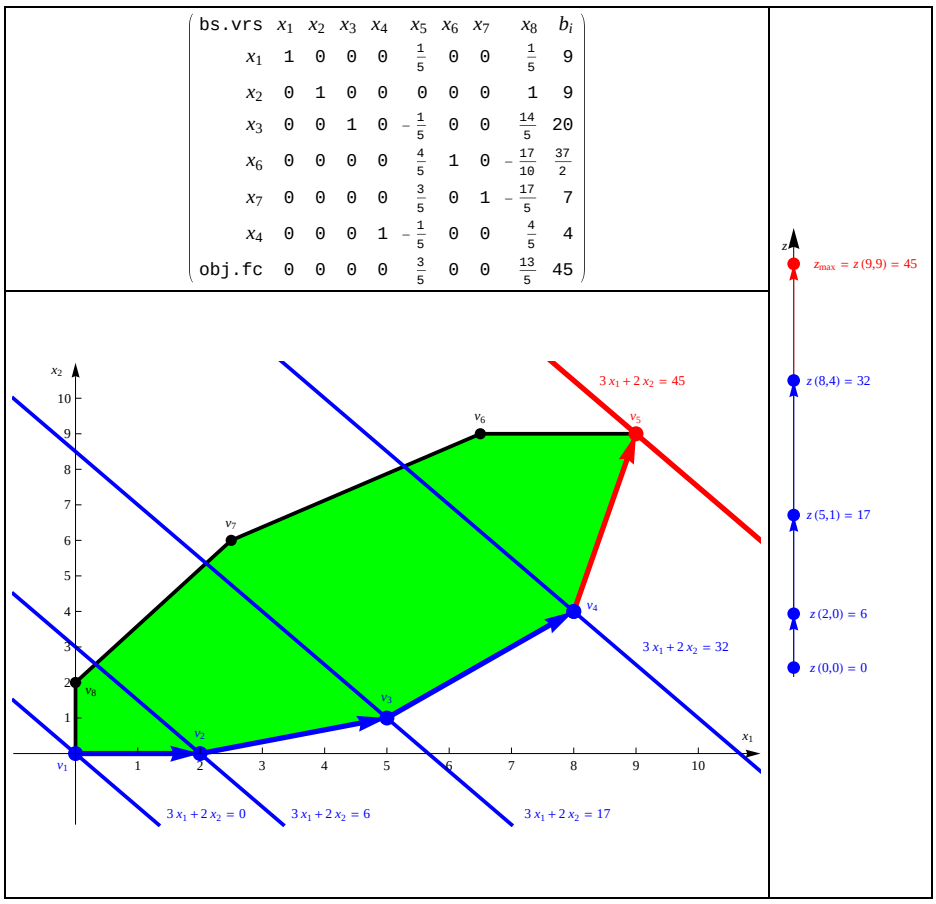


Figure 5: Fifth expanded Simplex Tableau.

The fifth expanded Simplex Tableau is optimal. We have: $z_{\max} = z(9,9) = 45$.

References

[1] Predrag S. Stanimirovic, Marko D. Petkovic, Milan Lj. Zlatanovic, *Visualization in optimization with Mathematica*, Filomat, 2009 23(2):68-81

[2] Bernard Kolman and Robert E. Beck, *Elementary Linear Programming with Applications*, 2nd ed., Academic Press, (1995)

[3] David G. Luenberger, *Linear and Nonlinear Programming*, 3rd ed., Springer, (2010)

[4] D. K. Liu, S.D. Huang, T.A. Brown, *Supporting Teaching and Learning of Optimisation Algorithms with Visualisation Techniques*, Proceedings of the 2007 AaeE Conference, Melbourne, (2007)

[5] Michael Bulmer and Michael Carter, *Integer programming with Mathematica*, The Mathematica Journal 1996, Miller Freeman Publication

[6] H. Ruskeepa *Mathematica Navigator: Graphics and Methods of applied Mathematics.* Academic Press, Boston (2005)

[7] S. Wolfram *The Mathematica Book.* Wolfram Media/ Cambridge University Press (1996)

Real-time animated dynamic geometry in the classrooms by using fast Gröbner basis computations

Z. Kovács[1]

[1] *The Private University College of Education of the Diocese of Linz, Austria, zoltan@geogebra.org*

The third millennium renaissance of elementary geometry by harnessing software applications in the classroom is already a history. By introducing dynamic geometry systems like *The Geometer's Sketchpad*, *Cabri* or *Cinderella* the high number of mechanical numerical computations enabled students to make their own experiments with geometric objects easy.

Today's computers go one step forward. Not only fast numerical computations are available, but symbolical commands help, for instance, to expand or factorize expressions or solve equations or even equation systems.

Nevertheless, application of symbolic computations in dynamic geometry remained an unexplored field for many years. Recent researches in the direction to compute Gröbner bases significantly faster than earlier[1], opened the road to manipulate on tens of equation systems in several variables within a second. Thus now it is possible to create real-time animations based on purely symbolic computations. Such real-time animations include computing locus or envelope equations for geometry constructions on various software platforms like native Java programs, web applications or mobile/tablet solutions.

In this scientific work the state of the art will be demonstrated in the *GeoGebra* dynamic mathematics tool which fully connects computer algebra and dynamic geometry. By computing and visualizing the algebraic equation of a non-trivial locus 29 frame per second (FPS) can be reached on an Intel(R) Core(TM) i7-2620M CPU @ 2.70GHz desktop computer (8 GB RAM installed, Ubuntu Linux 14.04.4). The same benchmark reaches 13 FPS as a web application in Google Chrome 49.0.2623.110.

Classroom application of the used technology is mainly on discovering general properties of geometry diagrams. GeoGebra—like many other DGS tools—makes it possible to construct a figure by using objects like points, lines or circles, and then, for example, GeoGebra's **LocusEquation** command calculates the equation of a locus (given by the tracer and mover points) and plots that as an implicit curve. When the user drags the free points of the diagram, the locus equation will be automatically recomputed using heavy symbolic computations, but due to the effectivity of the calculations, the equation will be obtained very quickly. Finally the

[1] See [10, 9] for two studies among the open source computer algebra systems.

implicit curve will be plotted by using numerical methods, based on the symbolical form of the equation. (See [8] for a more detailed explanation.)

A similar scenario is to create the envelope equation of a set of output paths while the moving point is bound to another object. (An envelope is a curve that is tangent to each member of the family of the output paths at some point.) Obtaining the envelope is possible by using the **Envelope** command in GeoGebra. More on this topic can be found in [7].

Recently another form of the **LocusEquation** command was introduced in GeoGebra, namely which calculates the locus of the free point such that a Boolean condition is satisified. This new form is also known as *implicit locus equation*. Due to the possibility to its direct use in the education, this third forms seems to be the most frequently used method to harness symbolic computations under the hood in a dynamic geometry experiment. For example, a natural way to discover Thales' theorem in the classroom is to construct a triangle *ABC* with GeoGebra, and then type the command `LocusEquation[`$a \perp b$`,`C`]`. In this way the circle with diameter *AB* will be immediately obtained and quickly redrawn when the free points *A* or *B* are dragged (Fig. 1).

All the three visualization activities above are common in using computational algebraic geometry to manipulate on coordinates of points, and their output is always an algebraic curve which is computed by—roughly speaking—eliminating some variables in the algebraic translation of the geometric construction. The elimination process is performed by the best available open source implementations, notably the standalone CAS *Singular* and the embedded system *Giac*.

The need to use symbolic computations instead of numerical ones in certain dynamic geometry visualization tasks is well discussed in the literature, see [5], section 3 for more details. All of the mentioned visualization activities are of the same kind.

The **LocusEquation** command was introduced in 2010 in GeoGebra's development version by the pioneer work of Botana's, Abánades', Escribano's and Arbeo's [4, 6], to translate the geometric construction into an algebraic equation system. The elimination step was implemented by outsourcing the computations to the computer algebra system *JAS* first, and later to *Reduce*, Singular and recently to Giac [10]. The visualization step of the locus equation as an implicit curve was implemented by Birklbauer and Drakulić [3] in 2011. Further improvements on the **LocusEquation** command were based on the joint work of the pioneers, and Montes' and Recio's [2].

Envelope support was added later by Botana and the author [5] in 2013. Implementation of the implicit locus equation was achieved by Abánades, Botana, Kovács, Recio and Sólyom-Gecse in 2016 (see [1] for a collection of examples).

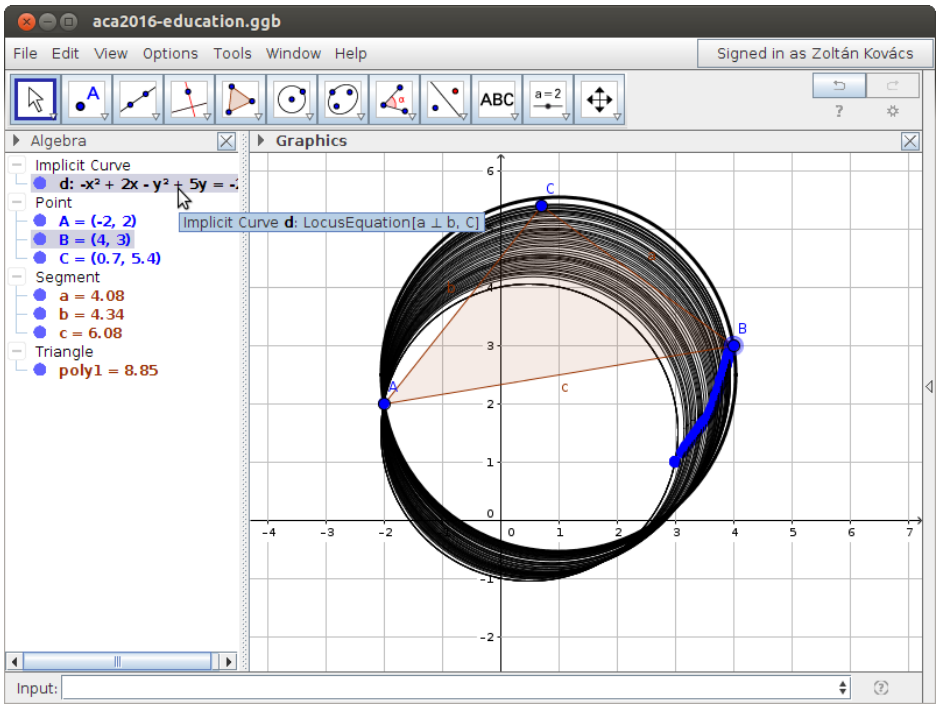


Figure 1: An imaginary classroom discovery of Thales' theorem while dragging point B from $(3,1)$ to $(4,3)$. Tracing is switched on for point B and implicit curve d. Here the animation reaches an average of 50 FPS for this simple theorem in desktop version of GeoGebra 5.0.237.0.

References

[1] M. Á. Abánades, F. Botana, Z. Kovács, T. Recio, C. Sólyom-Gecse, *Implicit loci*, `http://tube.geogebra.org/m/mbXQuvUV` (2016).

[2] M. Á. Abánades, F. Botana, A. Montes, T. Recio, *An algebraic taxonomy for locus computation in dynamic geometry*, Computer-Aided Design **56**, pp. 22-33 (2014).

[3] P. Birklbauer and D. Drakulić, *Implicit curves*. Second International GeoGebra Conference, Hagenberg, Austria. `http://ggbconference2011.pbworks.com/w/file/fetch/44873718/presentation.pdf` (2011).

[4] F. Botana and Z. Kovács, *Teaching loci and envelopes in GeoGebra*, `http://tube.geogebra.org/m/R8nUbEQV` (2014).

[5] F. Botana and Z. Kovács, *A Singular web service for geometric computations*, Annals of Mathematics and Artificial Intelligence, **74**, 3, pp. 359-370 (2015).

[6] F. Botana and Z. Kovács, *New tools in GeoGebra offering novel opportunities to teach loci and envelopes*. `https://arxiv.org/abs/1605.09153`, arXiv:1605.09153 [cs.CG] (2016).

[7] F. Botana and T. Recio, *Computing envelopes in dynamic geometry environments*, Annals of Mathematics and Artificial Intelligence, First online: 01 March 2016, pp. 1-18 (2016).

[8] Z. Kovács, *Loci problems in Age of Reason and their effect on GeoGebra – Locus equations and their factorization in GeoGebra*. International GeoGebra Conference, Budapest, Hungary. `http://test.geogebra.org/~kovzol/talks/igi14/bp.pdf` (2014).

[9] Z. Kovács, *Computer based conjectures and proofs in teaching Euclidean geometry*. PhD thesis, Johannes Kepler University, Linz, Austria (2015).

[10] Z. Kovács and B. Parisse, *Giac and GeoGebra – Improved Gröbner basis computations*, in *Computer Algebra and Polynomials, Volume 8942 of the series Lecture Notes in Computer Science*, pp. 126-138 (2015).

Familiarizing students with definition of Lebesgue integral - examples of calculation directly from its definition using Mathematica

Włodzimierz Wojas[1], Jan Krupa[2]

[1] *Warsaw University of Life Sciences (SGGW), Poland,* wlodzimierz_wojas@sggw.pl
[2] *Warsaw University of Life Sciences (SGGW), Poland,* jan_krupa@sggw.pl

"Young man, in mathematics you don't understand things. You just get used to them"

John von Neumann

In popular books of calculus, for example [1, 2], we can find many examples of Riemann integral calculated directly from its definition. The aim of these examples is to familiarize students with the definition of Riemann integral. But we cannot find analogical examples for Lebesgue integral. In this article, with similar aim but for Lebesgue integral definition, we present the following examples of calculation directly from its definition: $\int_0^1 x^2\,\mathrm{d}m(x)$, $\int_0^1 x^k\,\mathrm{d}m(x)$, $\int_0^{\pi/2} \sin x\,\mathrm{d}m(x)$, $\int_a^b \exp(x)\,\mathrm{d}m(x)$, $\int_0^{\pi} \ln(1-2r\cos x+r^2)\,\mathrm{d}m(x)$, where $\mathrm{d}m(x)$ denotes the Lebesgue measure on the real line. We calculate sums, limits and plot graphs of needed simple functions using Mathematica. The two following definitions of Lebesgue integral are used in this article:

Let $(\mathbb{R},\mathfrak{M},m)$ be measure space, where $\mathfrak{M}$ is $\sigma-$ algebra of Lebesgue measurable subsets in $\mathbb{R}$, and m- Lebesgue measure on $\mathbb{R}$.

Let $f:\mathbb{R}\to\mathbb{R}$ be measurable nonnegative function (we've omitted the definition of Lebesgue integral for simple real measurable functions).

Definition 1. (See [3, 5, 6, 7, 8])

$$\int f\,\mathrm{d}m(x)=\sup\Big\{\int s\,\mathrm{d}m(x) : 0\le s\le f, s \text{ simple measurable function}\Big\}. \quad (1)$$

Definition 2. (See [4, 9, 10]) Let s_n be nondecreasing sequence of nonnegative simple measurable functions such that $\lim\limits_{n\to\infty} s_n(x)=f(x)$ for every $x\in\mathbb{R}$. Then:

$$\int f\,\mathrm{d}m(x)=\lim_{n\to\infty}\int s_n\,\mathrm{d}m(x). \quad (2)$$

Example. Let consider the function: $f(x) = \sin x, x \in [0, \pi/2)$. For the rest of this example we will restrict our consideration to $x \in [0, \pi/2)$.

We will calculate $\int_0^{\pi/2} \sin x \, \mathrm{d}m(x)$ applying directly definition 1.

Consider

$\underline{s}_n(x) = \sum_{k=0}^{2^n-1} \sin\left(\frac{k}{2^{n+1}}\pi\right) \chi_{\left[\frac{k}{2^{n+1}}\pi, \frac{k+1}{2^{n+1}}\pi\right)}(x)$, for $x \in [0, \pi/2)$, $n = 1, 2, \ldots$

and $\bar{s}_n(x) = \bar{s}_n = \sum_{k=1}^{2^n} \sin\left(\frac{k}{2^{n+1}}\pi\right) \chi_{\left[\frac{k-1}{2^{n+1}}\pi, \frac{k}{2^{n+1}}\pi\right)}(x)$, for $x \in [0, \pi/2)$, $n = 1, 2, \ldots$.

Using Wolfram Mathematica we get the following Figures 1, 2:

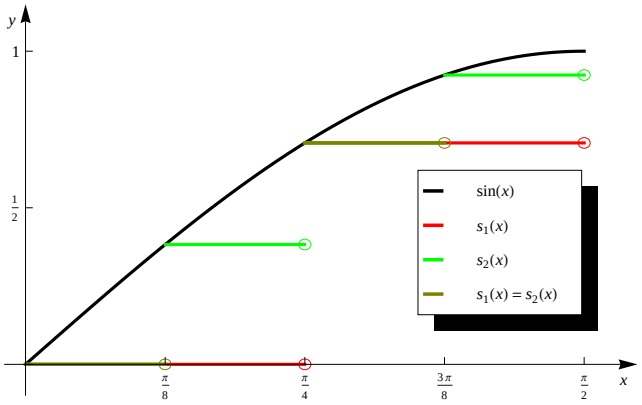


Figure 1: Graphs of functions $f, \underline{s}_1, \underline{s}_2$. We can see that $\underline{s}_1(x) \leq \underline{s}_2(x)$ for $x \in [0, \pi/2)$.

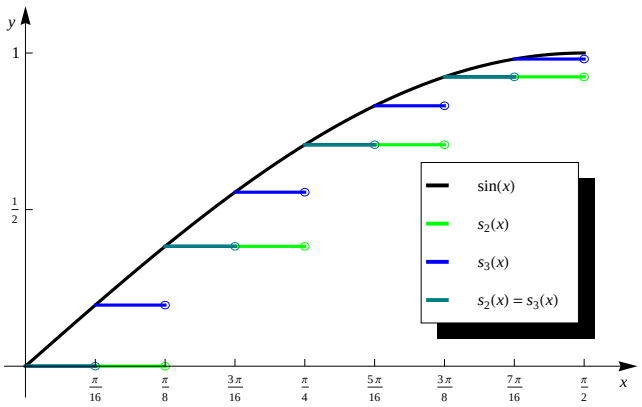


Figure 2: Graphs of functions $f, \underline{s}_2, \underline{s}_3$. We can see that $\underline{s}_2(x) \leq \underline{s}_3(x)$ for $x \in [0, \pi/2)$.

It is clear that $\underline{s}_n$, $\bar{s}_n$ are sequences of nonnegative simple measurable functions and that $\underline{s}_n \leq f$ and $\bar{s}_n \geq f$ on $[0, \pi/2)$ for all $n = 1, 2, \ldots$.

Using Wolfram Mathematica we get:

Listing 1: Mathematica code:

```
In[1]=Sum[Sin[Pi k/2^(n+1)], {k, 0, 2^n−1}] Pi/2^(n+1)//Simplify
Out[1]=2^(−2−n)Pi(−1+Cot[2^(−2−n)Pi])

In[2]=Limit[%,n−>Infinity]
Out[2]=1
```

So

$$\underline{a}_n = \int \underline{s}_n \, \mathrm{d}m)x) = \sum_{k=0}^{2^n-1} \sin \frac{k\pi}{2^{n+1}} \cdot \frac{1}{2^{n+1}} \pi = 2^{-2-n}\pi(-1 + \cot(2^{-2-n}\pi)) \to 1 \quad (3)$$

Similarly

Listing 2: Mathematica code:

```
In[3]=Sum[Sin[Pi k/2^(n+1)], {k, 1, 2^n}] Pi/2^(n+1)//Simplify
Out[3]=2^(−2−n)Pi(1+Cot[2^(−2−n)Pi])
```

```
In[4]=Limit[%,n->Infinity]
Out[4]=1
```

So

$$\bar{a}_n = \int \bar{s}_n \,\mathrm{d}m(x) = \sum_{k=1}^{2^n} \sin\frac{k\pi}{2^{n+1}} \cdot \frac{1}{2^{n+1}}\pi = 2^{-2-n}\pi(1+\cot(2^{-2-n}\pi)) \to 1 \qquad (4)$$

Of course we could use the following formulae: $\sum_{k=1}^{n} \sin(kx) = \frac{\sin\frac{n+1}{2}x \sin\frac{n}{2}x}{\sin\frac{x}{2}}$ and $\lim_{x\to 0}\frac{\sin x}{x} = 1$ instead of the code in Listings 1 and 2 to get the results in formulae (3) and (4).

Using formulae (3) and (4), basic properties of least upper, greatest lower bounds and of Lebesgue integral of simple measurable functions we will prove in our talk that:

$$\sup\left\{\int s\,\mathrm{d}m(x) : 0 \le s \le f, s \text{ simple measurable function}\right\} \ge 1 \qquad (5)$$

and

$$\sup\left\{\int s\,\mathrm{d}m(x) : 0 \le s \le f, s \text{ simple measurable function}\right\} \le 1. \qquad (6)$$

Inequalities (5) and (6) give

$$\sup\left\{\int s\,\mathrm{d}m(x) : 0 \le s \le f, s \text{ simple measurable function}\right\} = 1,$$

which means that $\int f\,\mathrm{d}m(x) = \int \sin x\,\mathrm{d}m(x) = 1$.

Let calculate $\int \sin x\,\mathrm{d}m(x)$ applying directly definition 2.

We can see that $\underline{s}_n(x) \le \underline{s}_{n+1}(x)$ for $x \in [0,\pi/2)$ and for all $n = 1,2,\ldots$. In Figures 1 and 2 we can see that $\underline{s}_1(x) \le \underline{s}_2(x)$ and $\underline{s}_2(x) \le \underline{s}_3(x)$ for $x \in [0,\pi/2)$. W can also see that $\lim_{n\to\infty} \underline{s}_n(x) = \sin(x)$ for all $x \in [0,\pi/2)$. So $\underline{s}_n$ is nondecreasing sequence of nonnegative simple measurable functions and $\underline{s}_n$ converges pointwise to f.

So by formula (3) and directly by definition 2 we get $\int \sin x\,\mathrm{d}m(x) = \int f\,\mathrm{d}m(x) = \lim_{n\to\infty}\int \underline{s}_n\,\mathrm{d}m(x) = \lim_{n\to\infty}\underline{a}_n = 1$.

References

[1] Tom M. Apostol, *Calculus, Volume 1, One-Variable Calculus with an Introduction to Linear Algebra*, 2nd ed., Addison-Wesley Publishing Company, (1991)

[2] G. M. Fichtenholz, *Differential and Integral Calculus*, Fizmatgiz, (1958)

[3] W. Rudin, *Principles of Mathematical Analysis*, 3rd ed., McGraw-Hill Education, (1973)

[4] Charalambos D. Aliprantis, Owen Burkinshaw, *Principles of Real Analysis*, 3rd ed., Academic Press, (1998)

[5] Robert G. Bartle, *The Elements of Integration and Lebesgue Measure*, Wiley-Interscience, (1995)

[6] Frank Jones, *Lebesgue Integration On Euclidean Space*, Jones & Bartlett Learning, (2000)

[7] Andrew Browder, *Mathematical Analysis An Introduction*, 2nd ed., Springer, (2001)

[8] Gerald B. Folland, *Real Analysis Modern Technique*, 2nd ed., Wiley, (2007)

[9] W. Kołodziej, *Mathematical Analysis*, (in polish), Polish Scientific Publishers PWN, Warsaw (2012)

[10] R. Sikorski, *Differential and Integral Calculus. Functions of several variables*, (in polish), Polish Scientific Publishers PWN, Warsaw (1977)

[11] H. Ruskeepa *Mathematica Navigator: Graphics and Methods of applied Mathematics.* Academic Press, Boston (2005)

[12] S. Wolfram *The Mathematica Book.* Wolfram Media/ Cambridge University Press (1996)

A framework for an ICT-based study of parametric integrals

Th. Dana-Picard[1], D. Zeitoun[2]

[1] *Jerusalem College of Technology, ndp@jct.ac.il*

[2] *Orot College for Education, ed.technologie@gmail.com*

Parametric definite integrals or, in other words, sequences of definite integrals, are important in various fields of mathematics and applied science. They are part of a standard curriculum for undergraduates, both in mathematics and science curricula.

In engineering science, such a parametric integral is often plotted as a family of curves depending on the parameter. A more efficient approach is to derive a mathematical formula for these integrals.

In most cases, an induction formula is found, using standard methods of integration, then methods for studying sequences are applied to derive a closed form for the integral, i.e. a form giving the integral as a function of the parameter. The easiest situation is encountered when, after the first integration step, the integrated term is equal to 0. Such a feature makes the usage of a telescopic method very efficient, whence formulas involving factorials and double factorials.

Sometimes, the integrand is too complicated for a regular student to be successful in computing the integral, even for small values of the parameter. In that case, a Computer Algebra System (CAS) may be used to perform the computation for a certain range of values of the parameter. A sequence of real values is created and used to conjecture a general formula. Now, instead of discovering a closed formula from scratch, the conjecture has to be proven. It is generally easier to check a conjecture than to derive a formula from scratch. Finding a good conjecture relies often on the usage of other Information and Communication Technologies (ICTs), such as online databases, in particular the Online Encyclopedia of Integer Sequences [5]. It provides formulas, references to literature, but also source code for the usage of a CAS. See also [3]. Searching these databases is valuable also for cases where the student can compute the integral, as it enables finding new connections with other mathematical fields.

Several Computer Algebra Systems, such as Maple, contain tutorials in order to help the user to perform specific tasks, for topics belonging to undergraduate syllabi (methods of integration, methods for the solution of differential equations, etc.).

For a given exercise, a built-in tutorial may propose different hints. Each one leads to a different pathway towards a solution, and the obtained expressions may

look different: a combinatorial expression, an infinite series, etc. Various identities have been proven by that way: integral identities, combinatorial identities, integral presentations of combinatorial objects, etc. For example, integral presentations of Catalan numbers are derived in [2] and of Stirling numbers in [4].

Numerous examples deal with a positive integer parameter, but it happens that the parameter is not limited to integers, but may be a non integer real number. Problems may appear with the possibilities of the CAS, depending on the mathematical theorems which have been implemented. For example, many CAS have hard time with the integral $I_r = \int_0^{\pi/2} \frac{1}{1+\tan^r x}\, dx$, when the parameter r is not an integer. Even if r is an integer, but not so small, the CAS may renounce to compute. Conversely, some CAS compute the integral with the general parameter and show that $I_r = \frac{\pi}{4}$ for every positive real r, using a theorem which appears rarely in textbooks (see [1]) .

In this talk, we show examples where a joint work with paper-and-pencil, CAS and online databases enable to derive important identities. As a byproduct, the usage of different ICTs enhances the existence of bridges between different domains of knowledge, in particular between continuous and discrete objects. We will show also an example where three different expressions obtained for the same parametric trigonometric integral (with non integer parameter) yield information for a problem in soil stability.

References

[1] Th. Dana-Picard (2005). *Parametric integrals and symmetries of functions*, Mathematics and Computer Education, 5-12.

[2] Th. Dana-Picard (2010): *Integral presentations of Catalan numbers*, International Journal of Mathematical Education in Science and Technology 41 (1), 63-69.

[3] R. Dickau (2010), *Stirling numbers of the second kind*, The Math Forum, Drexel University, http://mathforum.org/advanced/robertd/stirling2.html

[4] Th. Dana-Picard and D. Zeitoun (2012): *Sequences of definite integrals, infinite series and Stirling numbers*, International Journal of Mathematical Education in Science and Technology 43 (2), 219-230.

[5] N. J. A. Sloane (edt.): *The On-Line Encyclopedia of Integer Sequences*, published electronically at https://oeis.org

S3
Human-Computer Algebra Interaction

MATHCHECK2: Combining SAT and CAS

Curtis Bright[1], Vijay Ganesh[1], Albert Heinle[1], Ilias Kotsireas[2], Saeed Nejati[1], Krzysztof Czarnecki[1]

[1] *University of Waterloo, Waterloo, Canada*
{cbright,vijay.ganesh,aheinle,snejati,k2czarnecki}@uwaterloo.ca
[2] *Wilfrid Laurier University, Waterloo, Canada,*
ikotsire@wlu.ca

A recent important movement is the incorporation of modern solvers for satisfiability problems into suitable computations coming from the field of computer algebra. Projects like SC^2 [4] and publications like [1] demonstrate that the interest is coming from both academia and industry.

A great benefit of a combination of Computer Algebra Systems (CAS) and SAT solvers comes from the complementary strengths of both types of tools when utilized in synergy: The sophisticated search procedures and heuristics of modern SAT solvers combined with the domain specific knowledge provided by CASs.

With MATHCHECK [5], Vijay Ganesh and his student Edward Zulkoski presented the successful application of such a combination to problems coming from Graph theory, where they verified the Savage-Ruskey conjecture [7] up to a bound that has not been reached before. With MATHCHECK2 [6], we extended the functionality to deal with problems coming from combinatorics, in particular the search for practically relevant Hadamard matrices [2, 3]. Using state of the art techniques, we were able to scale to dimensions that were considered challenging before and found at least 160 Hadamard matrices, that had no equivalent entry in the MAGMA-database of Hadamard matrices.

By creating MATHCHECK2, we learned a structured approach on how to effectively use the SAT and CAS combination to counterexample/verify more mathematical statements in the future. We will report on our experiences, our results, and our vision how MATHCHECK2 may assist mathematicians to feasibly leverage the capabilities of SAT solvers together with computer algebra systems in their daily work to find non-trivial counter-examples or verifications for certain statements.

References

[1] Ábrahám, E.: Building bridges between symbolic computation and satisfiability checking. In: Proceedings of the 2015 ACM on International Symposium on Symbolic and Algebraic Computation. pp. 1–6. ACM (2015)

[2] Hadamard, J.: Résolution d'une question relative aux déterminants. Bull. sci. math 17(1), 240–246 (1893)

[3] Hedayat, A., Wallis, W., et al.: Hadamard matrices and their applications. The Annals of Statistics 6(6), 1184–1238 (1978)

[4] SC^2: Satisfiability checking and symbolic computation. `http://www.sc-square.org/`

[5] Zulkoski, E., Ganesh, V., Czarnecki, K.: MATHCHECK: A Math Assistant via a Combination of Computer Algebra Systems and SAT Solvers. In: Felty, A.P., Middeldorp, A. (eds.) Automated Deduction - CADE-25, Lecture Notes in Computer Science, vol. 9195, pp. 607–622. Springer International Publishing (2015)

[6] MATHCHECK2: A SAT+CAS Verifier for Combinatorial Conjectures. Under submission. `https://sites.google.com/site/uwmathcheck/`

[7] Ruskey, F. and Savage, C.: Hamilton cycles that extend transposition matchings in Cayley graphs of S_n. In: SIAM Journal on Discrete Mathematics,vol. 6, no. 1, pages 152–166, (1993)

Conservative conversion between LaTeX and TeXmacs [1]

Joris van der Hoeven[1], François Poulain[2]

[1] *LIX, CNRS, École polytechnique, Palaiseau, France, vdhoeven@lix.polytechnique.fr*
[2] *Amie, Coupelle Neuve, France, fpoulain@amie.coop*

Abstract

Back and forth converters between two document formats are said to be conservative if the following holds: given a source document D, its conversion D', a locally modified version M' of D' and the back conversion M of M', the document M is a locally modified version of D. We will describe mechanisms for the implementation of such converters, with the LaTeX and TeXmacs formats as our guiding example.

A.M.S. subject classification: 68U15, 68U35, 68N99
Keywords: Conservative document conversion, LaTeX conversion, TeXmacs, mathematical editing

1 Introduction

The TeXmacs project [10, 7] aims at creating a free scientific office suite with an integrated structured mathematical text editor [8], tools for graphical drawings and presentations, a spreadsheed, interfaces to various computer algebra systems, and so on. Although TeXmacs aims at a typesetting quality which is at least as good as TeX and LaTeX [14, 15], the system is not based on these latter systems. In particular, a new incremental typesetting engine was implemented from scratch, which allows documents to be edited in a wysiwyg and thereby more user friendly manner. This design choice made it also possible or at least easier to use TeXmacs as an interface for external systems, or as an editor for technical drawings. However, unlike existing graphical front-ends for LaTeX such as LyX [2] or Scientific Workplace [23], native compatibility with LaTeX is not ensured.

Since LaTeX is still the standard for scientific publications in areas such as mathematics, physics and computer science, good compatibility between TeXmacs and LaTeX is a major issue. Several use cases are possible in this respect. For the publication of papers, good converters from TeXmacs to LaTeX are a prerequisite. New TeXmacs users also would like to import their old LaTeX papers into TeXmacs. The most complex types of conversion arise when a TeXmacs user collaborates with a

person who refuses to use anything else but LaTeX. In that case, there is a need for lossless converters between both formats.

Unfortunately, TeX and LaTeX do not really provide a data format, but rather a programming language. Furthermore, unlike most other existing programming languages, the TeX system does not provide a formal grammar for the set of parsable documents. Moreover, the TeX syntax can be self-modified at run-time and many basic TeX/LaTeX capabilities are built upon syntactic tricks. This makes it extremely hard (or even impossible in practice) to design lossless converters between LaTeX and essentially different formats. Current software for conversions from LaTeX [5, 4, 13, 1, 18, 2, 17, 21, 16, 19, 20, 6, 11] therefore involves a lot of heuristics; we refer to section 3 for a quick survey of existing approaches.

Nevertheless, even if we accept that the conversion problem is hard in general, we would like our heuristic converters to address some important practical use cases. For instance, assume that Alice writes a LaTeX document and sends it to her colleague Bob. Now Bob makes a minor correction in the LaTeX document using TeXmacs and sends it back to Alice. Then Alice would like to recover her original LaTeX document except for the minor change made by Bob (which might possibly be exported in the wrong way). Converters between LaTeX and TeXmacs which admit this property will be called *conservative*.

There are several approaches to the implementation of conservative converters. First of all, we might re-implement our converters from scratch while taking into account the additional requirement. However, it took a lot of work and effort to develop the existing heuristic converters, so this option is not particularly nice from the implementers' perspective. Another idea would be to "hack" some parts of the existing code and turn it into something more conservative. Nevertheless, the existing converters are extremely complex; in particular, they cover numerous kinds of irregularities inside LaTeX. Adding an additional layer of complexification might easily break existing mechanisms.

Therefore, we want to regard the current converters between LaTeX and TeXmacs as black boxes. The aim of this paper is to describe conservative converters on top of these black boxes, which are currently under development. In particular, we guarantee that failure of the conservative converters only occurs in cases of failure of the original converters. Although our techniques were only tested for conversions between TeXmacs and LaTeX, it is likely that they can be used for other formats as well.

The first major ingredient for our converters (see section 4) is to generate, along with the main conversion, a correspondence between well chosen parts of the source document and their conversions in the target document. In particular, we want to track the image of each paragraph in the source document. Ideally speaking, assuming that we have a nice parse tree for the source document, we

want to track the images of all subtrees. In order to construct such correspondences, we will add markers to the source document, convert the marked source document, and finally remove the markers from the obtained marked target document. Optionally, we may want to verify that the addition and removal of markers does not disrupt the conversion process and that we obtain the same final document as in the case of a plain conversion.

For the conservative conversion itself, there are several approaches, which will be described in section 5. Our current implementations are mainly based on the "naive" approach from sections 5.1 and 5.2, which directly attempts to substitute unaltered document fragments by their original sources, when performing a back-conversion of a modified converted document. We are also experimenting with more elaborate approaches for which modifications are regarded as patches and where the idea is to lift the conversion process to such patches.

2 The LaTeX and TeXmacs document formats

2.1 The TeX and LaTeX formats

As we mentioned in the introduction, TeX [14] is really a programming language rather than a data format. The main emphasis of TeX is on presentation and typesetting quality. TeX programs are strings with a highly customizable syntax; the set of TeX primitives can also easily be extended with user defined macros. We recall that LaTeX [15] is a set of macros, built upon TeX. It is intended to provide an additional layer of structural markup, thereby allowing for a limited degree of presentation/content separation. It inherits both advantages and disadvantages from the TeX system.

One of the major disadvantages of TeX and LaTeX is that it is hard or even impossible to write reliable converters to other formats. For instance, in a recent case study on existing LaTeX to MathML converters [24], it turned out that the success rates of these converters varied between 2% and 54%, when applied to a large document base downloaded from ArXiv, and looking at the mathematical formulas only. There are numerous reasons for this poor performance. Let us briefly mention the main ones:

Lack of formal syntax. TeX documents do not comply to any well defined syntax, since the syntax can be modified at run time. For instance, it is rather easy to typeset an HTML snippet such as `<a href="#ex1" >example </a >` in the intended way using suitable TeX code. And, even though LaTeX widely advertises structured syntax, many LaTeX packages actually tweak TeX syntax in order to in-

clude external material (such as source code, algorithms, graphics) or to provide syntactic sugar, allowing to write code such as `foo!42!bar!!+++` (xcolor package) or `?[l]f*_ij^kl?` (tensid package). As a consequence, all existing parsers (except TEX-based parsers) are only able to correctly parse subsets of valid TEX documents.

Lack of semantics. The semantics of certain LATEX language constructs (such as `\csname` or `\expandafter`) may be hard to specify, and even harder to translate into other data formats. Indeed, it's quite usual to see code such as `\def\b{\begin}` or `\def\wd{\widehat}` in real life LATEX documents, which becomes meaningless when translated into a non-macro language (here, respectively due to the loss of the delimiter and to the loss of arity). LATEX is also dramatically lacking in "public interfaces". So much so that many customisations are done using side effects, by redefining internal macros. So again, all existing translators are only able to translate subsets of valid TEX documents.

Lack of orthogonality. LATEX, as a document format, is dramatically lacking in orthogonality. Numerous packages are mutually incompatible and numerous document classes provide different macro naming conventions, making code non portable between classes (*e.g.* the declaration `\newtheorem{thm}{Theorem}` may be used with the article class, but is forbidden with elsart). Numerous macros suffer from arbitrary limitations (*e.g.* a paragraph cannot end inside a `\texttt` argument; the nesting level in lists is limited to 4, etc.). Each document class defines its very own scheme for defining metadata and title pages. The characters `<`, `>` and `|` behave very differently depending on the preamble. Etc. All these irregularities make it difficult to build generically valid LATEX documents.

2.2 The TEXMACS format

The TEXMACS document format is based on *trees*: all TEXMACS documents or document fragments should be thought of as trees [9]. Of course, such trees can be serialized as strings in different ways: as XML documents, as SCHEME expressions (S-expressions), etc. In what follows, we will represent TEXMACS trees using S-expressions. Figure 1 shows an example of a TEXMACS snippet.

In the example, the `concat` tag stands for "horizontal concatenation" and its children expect "*inline* content". Another important primitive which will be used in subsequent examples is `document`; this tag is used for "vertical concatenation" and it provides "*block* content".

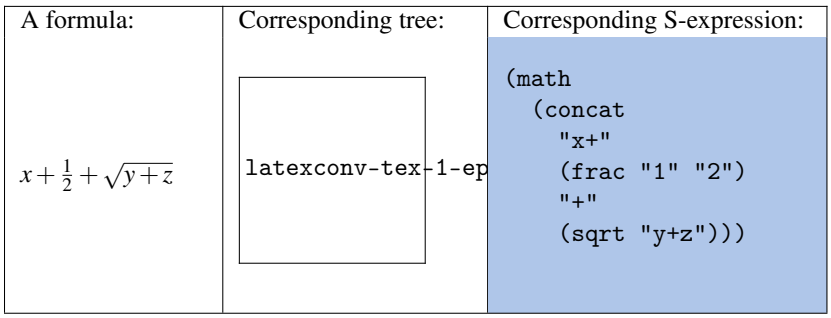


Figure 1: An insight of the $\TeX_{\text{MACS}}$ format.

3 Traditional converters for LaTeX

3.1 Existing approaches

Not so surprisingly, the interoperability with LaTeX is an asymmetric problem. Conversion to LaTeX is considered the easier problem, since we are free to restrict ourselves to a subset of LaTeX. However, even this problem is quite non trivial, due to lack of orthogonality and arbitrary restrictions inside LaTeX (see section 2.1). Nevertheless, conversion from LaTeX to other formats is indeed the most difficult problem, usually. Although the techniques described in this paper work both ways, we will therefore use this harder direction for our examples.

The main obstacle when converting LaTeX documents to other formats is that arbitrary LaTeX documents are hard to parse. One way to bypass this problem is to let TeX do the parsing for you. Some existing converters which use this approach are TeX4HT, LXIR, HERMES and LaTeXML [5, 13, 1, 18]. The underlying principle is to build an overloaded DVI document [3, 22] with additional markup which delimits the scope of a set of interesting macros. Then, via an external program, it is possible to rebuild a tree reflecting the structure of the original document. This alternative has the very benefit of exploiting the TeX parser without rewriting it, but it has also major concerns:

1. It supposes that you installed a complete TeX distribution (usually large in size), whose version is compatible with the one required by the source.

2. It only works for complete documents, and not for code snippets.

3. User defined macros are expanded and thereby lose their semantics.

Concerning the last point, we agree with [12]: “macro expanding then translating is best suited to display and does not provide converted documents suitable for further

use", so this strategy does not fit our needs. Also, even if we could preprocess sources in order to protect user defined markup, the two first concerns are too restrictive for our project.

The remaining strategy is to parse the LaTeX source files ourselves. This approach has been followed by software such as LyX, HeVeA, PlasTeX, Tralics, Pandoc, Latex2html, Perl LaTeX::Parser, HyperLaTeX, TtH, etc. [2, 4, 17, 21, 16, 19, 20, 6, 11] Once the document parsed, a tree is generated and is transformed in order to comply with the target format definition.

3.2 Traditional conversion from LaTeX to TeXmacs

The existing LaTeX to TeXmacs converter uses a custom TeX/LaTeX parser, with the ability to conserve the semantics of user defined macros. Many filters are applied to the parsed LaTeX document in order to get a suitable TeXmacs tree. Some example transformations which are applied are the following:

- expansion of "dangerous" macros, such as `\def\b{\begin}`;
- cutting the source file into small pieces, thereby reducing the risk of serious parse errors due to (text/math) mode changes;
- many local and global tree rewritings (whitespace handling, basic normalizations and simplifications, renaming nodes, reordering children, migrating label definitions, extracting metadata, etc.);
- adding semantics to mathematical content (disambiguation of operators and whitespace, matching delimiters, etc.);
- (optionally) compile the LaTeX document with the preview package in order to import hard-to-parse document fragments as pictures.

Due to the combined complexity of these transformations, we cannot make certain useful assumptions on the behavior of our converter, especially:

(non) Linearity The conversion of a concatenation of snippets might not be the concatenation of the conversion of the snippets.

(non) Locality Local changes inside snippets may result in global changes.

(non) Time invariance Two conversions of the same document at different times might result in different results. This is for instance due to time stamping by external tools involved in the conversion of pictures.

3.3 Traditional conversion from TeXmacs to LaTeX

The converter from TeXmacs to LaTeX does not have to cope with the LaTeX parsing problem. Nevertheless, arbitrary restrictions inside LaTeX and the general lack of orthogonality make the production of high quality LaTeX documents (including preserved semantics of user defined macros) harder than it seems. The LaTeX export process is based on the following general ideas:

- converting the document body tree into a LaTeX syntax tree;
- building the preamble by tracking dependencies and taking into account all document style options;
- writing the preamble and the body.

Again, and for similar reasons as above, useful properties such as linearity, locality and time invariance cannot be guaranteed.

4 Correspondence between subdocuments

4.1 Basic principles

One important prerequisite for conservative converters is our ability to maintain the correspondence between parts of the source document and their images in the target document. When writing conservative converters from scratch, this correspondence can be ensured by design. In our setting, since traditional converters are already written, we consider them provided as if they were black boxes, independant from our conservative converters. Then, the key idea in order to maintain the correspondence between source and target is to add markers to the source document before doing the conversion. More precisely, we extend the source and target formats with one new special tag for marking text, say `marker`. Two design choices have now to be made.

First of all, the `marker` tag can either be punctual or scoped. In the first case, the tag takes a unique identifier as its single argument. In the second case, the tag takes the marked text as its additional second argument (for large multi-paragraph fragments of LaTeX, this requires `marker` to be an environment). For unparsed LaTeX source documents, substrings which correspond to logical subexpressions of the parse tree can be hard to determine. Consequently, punctual markers are most adequate for the initial conversions from LaTeX to TeXmacs. Nevertheless, using a post treatment, we will show in section 4.2 below that punctual markers may be grouped by pairs into scoped markers, while taking advantage of the tree structure

of the generated TEXMACS document. For conversions from TEXMACS to LATEX, we may directly work with scoped markers.

Secondly, we have to decide on the granularity of our conservative converters: the more markers we use, the more locality will be preserved for small changes. However, not all subtrees of the parse tree of the source document necessarily give rise to valid subexpressions of the target documents. Moreover, in the case of conversions from LATEX to TEXMACS, we have no direct access to the parse tree of the source document, so appropriate places for markers have to be chosen with care. At least, we need to mark all paragraphs. More sophisticated implementations will also mark macro definitions in the preamble, cells of tables, and several well chosen commands or environments.

Example 1 In Figure 2, we have shown a simple example of added punctual markers inside a LATEX source document. The granularity is slightly better than a purely paragraph based marking with which the markers 4 until 9 would be suppressed. Nevertheless, an even better granularity could for instance be obtained by putting markers around the `b` and `c` of the fraction. As a post treatment we typically group the punctual markers by pairs into scoped markers. In this case, the pairs are $(1,2)$, $(3,10)$, $(4,7)$, $(5,6)$, $(8,9)$ and $(11,12)$.

```
First paragraph.

%Some comments
\begin{remark}
 Some mathematics
 \[ a+\frac{b}{c}. \]

 More text.
\end{remark}

Last paragraph.
```

$\rightsquigarrow$

```
\marker{1}First paragraph.\marker{2}

%Some comments
\marker{3}\begin{remark}
  \marker{4}Some mathematics
  \[ \marker{5}a+\frac{b}{c}.\marker{6} \]\marker{7}

  \marker{8}More text.\marker{9}
\end{remark}\marker{10}

\marker{11}Last paragraph.\marker{12}
```

Figure 2: Rudimentary example of a marked LATEX source document body.

4.2 Grouping punctual markers by pairs

In order to transform matching pairs of punctual markers inside LATEX source documents into scoped markers, we will make use of the tree structure of the marked TEXMACS target document obtained after conversion.

Roughly speaking, for every subtree which starts with marker i and ends with marker j, we declare that (i, j) forms a matching pair. More precise implementa-

tions should carefully take into account the special nature of certain tags such as `concat` and `document`. For instance, we may use the following algorithm:

- any `concat` tag or `document` tag starting and finishing by a marker is replaced by the corresponding pair;
- any child of a `concat` tag or a `document` tag which is framed by two markers is replaced by the corresponding pair;
- any `concat` tag or `document` tag with only one child which is a pair is replaced by the pair;
- any remaining marker is removed.

Example 2 For the simple document from Example 1, the TEXMACS conversion of the marked document would be as follows:

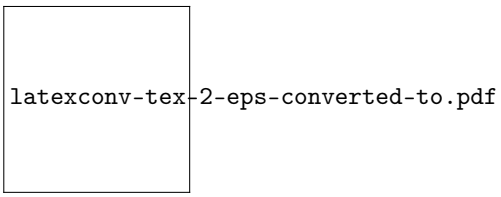
```
(document
  (concat (marker "1")) "First paragraph." (marker "2")))
  (marker "3"))
  (remark
    (document
      (concat (marker "4")) "Some mathematics")
      (equation*
        (document (concat (marker "5")) "a+" (frac "b" "c") "." (marker "6")))))
      (marker "7"))
      (concat (marker "8")) "More text." (marker "9")))))
  (marker "10"))
  (concat (marker "11")) "Last paragraph." (marker "12"))))
```

The pairs $(1,2)$, $(5,6)$, $(8,9)$ and $(11,12)$ are detected as matching pairs of markers of inline content, whereas the pair $(3,10)$ is detected as matching pair of block content. The pair (4,7) does not match, but the matching algorithm can be further tweaked to better handle this kind of situations.

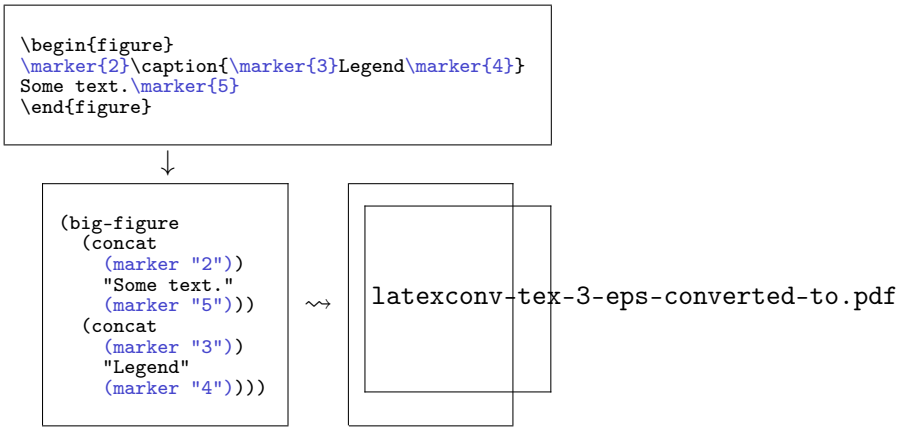
At a second stage, we may organize the matching pairs into a dag: a pair (i,j) will be a descendent of a pair (p,q) whenever the source string corresponding to (i,j) is included in the source string corresponding to (p,q). We will say that the dag is *well formed* if it is actually a tree and whenever the source strings corresponding to two different children of the same node never intersect.

Example 3 For our example document, and adding an implicit pair $(0,13)$ for the

root, the dag of matching pairs is a well formed tree:



Example 4 Certain tags, such as `figure`, may produce badly formed trees:



In unfavourable cases, such as Example 4, the dag of matching pairs does not yield a well formed tree. In such cases, we keep removing offending matching pairs until we do obtain a well formed tree. At the end of this process, we are ensured that marked subdocuments do not overlap in non structured ways, i.e. other than *via* inclusion. Consequently, it is possible to transform the document with punctual markers into a document with scoped markers.

Example 5 Applying the final transformation to Example 2, we obtain the document below. Of course, the names of our scoped identifiers can be replaced by simple numbers.

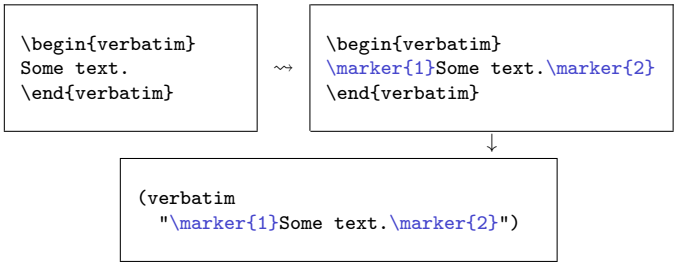
```
(document
  (marker "1:2" "First paragraph.")
  (marker "3:10"
    (remark
      (document
        "Some mathematics"
        (equation*
          (document (marker "5:6" (concat "a+" (frac "b" "c") "."))))))
```

```
    (marker "8:9" "More text.")))
 (marker "11:12" "Last paragraph." ))
```

4.3 Detection and reparation of irregularities

In most cases, removal of the markers from the conversion of a marked source document yields the same result as the direct conversion of the source document, modulo some normalization, such as merging and removing `concat` tags. However, this is not always the case. Let us give a few examples of how this basic principle may fail.

Example 6 When putting markers inside certain special tags, such as `verbatim`, the markers may not be converted as expected:



Example 7 The conversion of certain LaTeX documents may involve some restructuring which is incompatible with the marking algorithm. For instance, TeXmacs only allows for modified text properties of block content if the modified properties apply to a succession of entire paragraphs. LaTeX also allows emphasized text which starts in the middle of a paragraph, runs over several subsequent paragraphs, and then ends in the middle of another paragraph. When importing this kind of ill structured emphasized text, we therefore restructure the emphasized text into three separate parts. However, such transformations often interfere in unpredictable ways with the marking process.

In order to guarantee that our marking and unmarking mechanisms never deteriorate the quality of the converters, we may use the following simple procedure: convert the source document both with and without the marking/unmarking mechanism. If the results are the same, then return the result. Otherwise, keep locating those markers which are responsable for the differences and put them into a blacklist. Now keep repeating the same process, while no longer inserting the markers in the blacklist during the marking procedure. In the worst case, this process will put all markers on the blacklist, in which case conversion with and without the marking/unmarking mechanism coincide.

4.4 Conservative storage of documents

In order to allow for subsequent conservative back and forth conversions, the result of a conservative conversion should contain additional information on how the recover the original source file. More precisely, when converting a source document D from format A into format B, the target document will consist of a quadruple $(D', \bar{D}, \bar{D}', \lambda)$, where

- D' is the target document of format B.
- $\bar{D}$ is the marked source document which gave rise to the marked version $\bar{D}'$ of the target document.
- λ is a mapping which associates snippets from one of the two formats A or B to every identifier for a marked subdocument.

If our target format is TeX$_{\text{MACS}}$, then we simply store $\bar{D}$, $\bar{D}'$ and λ as attachments to TeX$_{\text{MACS}}$ files. If LaTeX is our target format, then, by default, we put $\bar{D}$, $\bar{D}'$ and λ inside a comment at the end of the document. Alternatively, we may store $\bar{D}$, $\bar{D}'$ and λ in a separate file, which will be consulted whenever we convert a modification of the target document back to A. The last strategy has the advantage that we do not clobber the converted file. However, one will only benefit from the conservative converters when the LaTeX reimportation is done on the same computer and *via* the same user account.

Remark 1 Instead of specifying λ as a separate mapping, it also possible to suffix identifiers for marked subdocuments by a letter for the original format of the marked text.

Example 8 When importing the LaTeX source file from Examples 1 and 5 into TeX$_{\text{MACS}}$, the mapping λ will associate "LaTeX" to each of the identifiers `1:2`, `3:10`, `5:6`, `8:9`, `11:12`. If the LaTeX source file was a modified version of the result of exporting a TeX$_{\text{MACS}}$ file to LaTeX, then the mapping λ will associate TeX$_{\text{MACS}}$ to every node of the tree, except for those nodes which correspond to substrings in which modifications took place.

5 Conservative conversion

5.1 The naive approach

Let us return to the main problem of conservative conversion. Alice has written a document D in format A, converts it to format B and gives the resulting document

D' to Bob. Bob makes some modifications and sends a new version M' back to Alice. How to convert the new version back to format A while conserving as much as possible from the original version for the unmodified parts?

Let us first describe a naive solution to this problem. We will assume that the format B is enriched with one new unary tag `invariant`, with an expression of format A as its unique argument. The conversion from B to A of such a tag will be precisely this argument.

In the light of the section 4.4, Bob's new version contains a marked copy $\bar{D}$ of Alice's original version as well as its marked conversion $\bar{D}'$ to format B. Now for every subdocument S' occurring in M' which corresponds to a marked subdocument of $\bar{D}'$ (and which is maximal with this property), we replace S' by an `invariant` tag which admits the subdocument S in D corresponding to S' as its argument. We finally convert the obtained document from B to A using our slightly adapted black box converter.

Example 9 Assume that Bob adds two more dots to the paragraph `More text.` in Example 2. Then the subdocuments corresponding to the pairs of markers $(1,2)$, $(5,6)$ and $(11,12)$ still occur in the new document. Since $(8,9)$ corresponds to a subdocument of $(3,10)$, we only declare the subdocuments corresponding to $(1,2)$, $(5,6)$ and $(11,12)$ to remain invariant. More precisely, we perform the conversion

```
(document
(invariant "First paragraph.")
  (remark
    (document
      (invariant "Some mathematics
      \[ a+\frac{b}{c}. \]")
 "More text..."))
        (invariant "Last paragraph."))
```

$\rightsquigarrow$

```
First paragraph.

\begin{remark}
  Some mathematics
 \[ a+\frac{b}{c}. \]

  More text...
\end{remark}

Last paragraph.
```

Notice the change of indentation and the disappearance of the comment.

5.2 Fine tuning of the naive approach

A few additional precautions are necessary in order to make the naive approach fully work. First of all, during the replacement procedure of subdocuments S' of M' by invarianted subdocuments S of D, some subdocuments S' of M' might correspond to several marked subdocuments $S_1, \ldots, S_n$ of D. In that case, we first investigate some of the context in which S' occurred, such as the first $k = 1, 2, \ldots$ marked subdocuments before and after S'. In many cases, there will be only one

subdocument S_i which will both correspond to S' and its context. If such a preferred match S_i cannot be found for S', then we renounce replacing S' by an invariant tag.

Secondly, the conversion algorithms are allowed to be context dependent. For instance, ordinary text and mathematical formulas are usually not converted in the same way. When replacing subdocuments S' of M' by invarianted subdocuments S of D, we thus have to verify that the context of S' in M' is similar to the context of S' in D'.

Some other improvements can be carried out in order to further improve the quality of naive conservative conversions. For instance, in Example 9, we observed that the comment before the remark is lost. This would not have been the case if Bob had only modified the last paragraph. It is good practice to detect adjacent unchanged portions of text and keep the comments in the corresponding parts of the original source file, but it may be difficult to achieve.

Additional *ad hoc* techniques were used to solve others problems. For instance, certain editors automatically damage the line breaking of LaTeX source code. This issue has been addressed by normalizing whitespace before testing whether two subdocuments are identical.

5.3 Patch based conservative conversions

Another strategy towards conservative editing is to determine the changes between the conversion S' of Alice's version and Bob's version D' in the form of a "patch" π', and then try to convert this patch π' into a patch π that can be applied to S. Before anything else, this requires us to fix formats $A^\sharp$ and $B^\sharp$ for the description of patches for the formats A and B.

For instance, LaTeX documents are strings, so LaTeX patches could be sets of triples (i, j, R), where $(i, j) \in \mathbf{N}^2$ corresponds to a substring of the source string and R stands for a replacement string for this substring. This language might be further extended with pairs $((i_1, \ldots, i_n), \sigma) \in \mathbf{N}^n \times \mathfrak{S}_n$, where $(i_1, \ldots, i_n)$ is an n-tuple of positions $0 \leqslant i_1 < \cdots < i_n \leqslant l$ of the source string (of length l) and σ a permutation. The patch then applies the permutation σ to the substrings $(0, i_1), (i_1, i_2), \ldots, (i_n, l)$ of the source string.

Similar patches can be used for TeXmacs trees, by operating on the children of a node instead of the characters in a string. In TeXmacs, we also implemented a few other types of elementary patches on trees for the insertion or removal of new nodes and splitting or joining nodes. However, we have not yet used these more complex kind of patches in our conservative converters. In general, we notice that richer patch formats lead to more conservative converters, but also make implementations more complex.

Let us study the most important kind of patches π' which simply replaces a

subdocument X' of D' by Y'. If X' is marked inside $\bar{D}'$, with X as the corresponding source in D, then we take π to be the replacement of X by contextual conversion Y of Y' into format A. This contextual conversion of Y' is obtained by performing a marked conversion of M' into format A and then look for the conversion of Y' as a subdocument of M'.

Example 10 Assume again that Bob adds to more dots to the paragraph `More text.` in Example 2. Then π' is the patch which replaces subtree `"More text."` by `"More text..."`. This subtree `"More text."` corresponds to the pair of markers $(8,9)$ and to the unique substring `More text.` in the original source document. Consequently, π will be the patch which replaces this substring by `More text...`, which leads to the conservative conversion

```
First paragraph.

%Some comments
\begin{remark}
 Some mathematics
 \[ a+\frac{b}{c}. \]

 More text...
\end{remark}

Last paragraph.
```

5.4 Fine tuning of the patch based approach

Several things have to be fine tuned for the patch based approach. Example 10 is particularly simple in the sense that the patch π' which replaces `"More text."` by `"More text..."` replaces a subtree by another tree. More generally, we have to consider the case when a succession of children of a subtree is replaced by a sequence of trees. This occurs for instance when inserting or deleting a certain number of paragraphs. For special types of nodes (such as the TEXMACS `document` tag for successions of paragraphs), we know how the node behaves under conversions, and we can devise an *ad hoc* procedure for computing the patch π. In general however, we may have to replace π' by a less fine grained patch which replaces the entire subtree by a new tree.

A similar situation arises when the patch π' replaces as subdocument X' of D' which is not marked inside $\bar{D}'$, or when the subdocument Y' of M' does not lead to marked subdocument D of the marked conversion of M' into format A. In these cases as well, a simple solution again consists of replacing π' by a less fine grained patch which replaces a larger subtree by another tree.

Example 11 In Example 2, assume that Bob replaces the numerator `b` of the fraction by `x`. This corresponds to a patch π' which does not operate on a marked subtree of $\bar{D}'$. Nevertheless, the patch which replaces the marked subtree `(concat "a+" (frac "b" "c"))` by `(concat "a+" (frac "x" "c"))` does admit the required form.

5.5 The combined approach

The quality of conservative converters can be further enhanced by combining the naive and patch based approaches. Assume that M' is obtained from D' through the application of a set $\pi'_1, \ldots, \pi'_n$ of independent patches (i.e., acting on disjoint subdocuments of D'). If $n > 0$, then we will reduce the general "patch conversion" problem to a problem of the same kind but with a strictly smaller number of patches n'.

Consider a subdocument S' of D' with the following properties:

- The subdocument is marked inside $\bar{D}'$ and corresponds to the subdocument S of D.
- At least one of the patches π'_i applies to a part of S'.
- S' admits no strictly smaller subdocuments satisfying the same properties.

Let T' be the result of applying all relevant patches π'_i to S'. Now apply the marked version of the naive conversion techniques from sections 5.1 and 5.2 to M'. This will yield a conservative contextual conversion T of T' into format A.

We now consider the new "source document" D^* obtained from D through the replacement of S by T. Similarly, we consider the new "conversion" D'^* obtained from D' through the replacement of S' by T'. These replacements admit marked versions which basically change nothing outside S and S' and remove all markers strictly inside S and S'. This completes our reduction of the general "patch conversion" problem to one with strictly less patches (namely, all remaining patches which did not apply to S'). In practice, several non overlapping subdocuments S' can be treated in a single iteration, so as to increase the efficiency.

6 Conclusion

Conservative converters should make collaborations easier between people who are working with different authoring tools. Although we only considered conversions between TeXmacs and LaTeX here, our methods should also be useful for other

formats. We also notice that the approach generalizes in a straightforward way to the documents which are written using three or more different tools or formats.

The implementations inside TEXMACS have only started quite recently and some time will still be needed for testing and maturing. Nevertheless, our first experiences are encouraging. Currently, we are still struggling with conservative conversions of user defined macros and metadata such as title information. Nevertheless, we are confident that a suitable solution can be worked out even for complex conversion challenges of this kind, by finetuning the grain of our marking algorithm, and through the progressive integration of the patch based approach.

References

[1] Romeo Anghelache. Hermes. `http://hermes.roua.org/`, 2005.

[2] M. Ettrich et al. The LyX document processor. `http://www.lyx.org`, 1995.

[3] David Fuchs. The format of TEX's DVI files. *TUGboat*, 3(2):13–19, 1982.

[4] José Grimm. Tralics. `http://www-sop.inria.fr/marelle/tralics/`, 2003.

[5] E. Gurari. TeX4ht: LATEX and TEX for hypertext. `http://www.tug.org/applications/tex4ht/mn.html`, 2010.

[6] Sven Heinicke. LaTeX::Parser – Perl extension to parse LATEX files. `http://search.cpan.org/~svenh/LaTeX-Parser-0.01/Parser.pm`, 2000.

[7] J. van der Hoeven. GNU TEXmacs: A free, structured, wysiwyg and technical text editor. In Daniel Filipo, editor, *Le document au XXI-iÃ¨me siÃ¨cle*, volume 39–40, pages 39–50, Metz, 14–17 mai 2001. Actes du congrÃ¨s GUTenberg.

[8] J. van der Hoeven. Towards semantic mathematical editing. Technical report, HAL, 2011. `http://hal.archives-ouvertes.fr/hal-00569351`, submitted to JSC.

[9] J. van der Hoeven. *GNU TEXmacs User Manual*, chapter 14: The TEXmacs format. HAL, 2013. `http://hal.archives-ouvertes.fr/hal-00785535`.

[10] J. van der Hoeven et al. GNU TEXmacs. `http://www.texmacs.org`, 1998.

[11] Ian Hutchinson. TtH, the TEX to html translator. http://hutchinson.belmont.ma.us/tth/, 1997.

[12] Rodionov I. and S. Watt. A TeX to MathML converter. http://www.orcca.on.ca/MathML/texmml/textomml.html.

[13] Jean-Paul Jorda and Xavier Trochu. LXir. http://www.lxir-latex.org/, 2007.

[14] D.E. Knuth. *The TeXbook*. Addison Wesley, 1984.

[15] L. Lamport. *LATEX, a document preparation system*. Addison Wesley, 1994.

[16] J. MacFarlane. Pandoc: a universal document converter. http://johnmacfarlane.net/pandoc/index.html, 2012.

[17] L. Maranget. HeVeA. http://para.inria.fr/~maranget/hevea/index.html, 2013.

[18] B. Miller. LATEXML: A LATEX to XML converter. http://dlmf.nist.gov/LaTeXML/, 2013.

[19] R. Moore. LATEX2HTML. http://www.latex2html.org, 2001.

[20] T. Sgouros. HyperLaTeX. http://hyperlatex.sourceforge.net, 2004.

[21] Kevin Smith. plasTEX. http://plastex.sourceforge.net/, 2008.

[22] M. Sofka. TEX to HTML translation via tagged DVI files. *TUGboat*, 19(2):214–222, 1998.

[23] MacKichan Software. Scientific workplace. http://www.mackichan.com/index.html?products/swp.html~mainFrame, 1998.

[24] H. Stamerjohanns, D. Ginev, C. David, D. Misev, V. Zamdzhiev, and M. Kohlhase. MathML-aware article conversion from LATEX, a comparison study. In P. Sojka, editor, *Towards Digital Mathematics Library, DML 2009 workshop*, pages 109–120, Masaryk University, Brno, 2009. http://kwarc.info/kohlhase/papers/dml09-conversion.pdf.

Math Web Search Interfaces and the Generation Gap of Mathematicians

A. Kohlhase[1]

[1] *University of Applied Sciences, Neu-Ulm, Germany*

New technologies and interfaces are changing the way users engage with technology, mathematicians are no exception. In a previous study we found some interesting attitudes/practices of professional mathematicians with respect to search interfaces, that sets them apart from other web searchers. In a nutshell, this study explores whether and if so, how math search interfaces are distinctly perceived by younger and older mathematicians and we offer first design implications.

Collaborative Computer Algebra Shell

M. Minimair[1]

[1] *Seton Hall University, South Orange, New Jersey, USA, minimair@shu.edu*

Even though team work is very common in applied computer algebra, mathematics and scientific research, software for computational mathematics often lacks sufficient support for collaborators [2] who want to solve problems together. The current ongoing project focuses on enhancing collaborative use of computer algebra shells [1] by multiple users connected online. The collaborative shell environment, devoloped by the project, is based on the Jupyter/iPython framework [4, 5] and tightly integrates chat messages [3] with mathematical command execution. This integration enables the collaborators to interact while jointly developing computational scripts and serves to document the collaborative process when solving problems.

References

[1] Christopher Brown, Hans-Wolfgang Loidl, Jost Berthold, and Kevin Hammond. Improving your cash flow: the computer algebra shell. In *Implementation and Application of Functional Languages*, pages 169–184. Springer, 2010.

[2] Andrea Bunt, Michael Terry, and Edward Lank. Challenges and opportunities for mathematics software in expert problem solving. *Human–Computer Interaction*, 28(3):222–264, 2013.

[3] Hugo Fuks, Mariano Pimentel, and Carlos José Pereira De Lucena. RU-Typing-2-Me? evolving a chat tool to increase understanding in learning activities. *International Journal of Computer-Supported Collaborative Learning*, 1(1):117–142, 2006.

[4] Fernando Pérez and Brian E Granger. IPython: a system for interactive scientific computing. *Computing in Science & Engineering*, 9(3):21–29, 2007.

[5] M. Ragan-Kelley, F. Perez, B. Granger, T. Kluyver, P. Ivanov, J. Frederic, and M. Bussonier. The Jupyter/IPython architecture: a unified view of computational research, from interactive exploration to communication and publication. *AGU Fall Meeting Abstracts*, December 2014.

S4
Applied and Computational Algebraic Topology

Computing Betti numbers of Veronese subrings with Pommaret bases

Matthias Fetzer[1]

[1] *Universität Kassel, Germany, fetzer@mathematik.uni-kassel.de*

Involutive bases, and in particular Pommaret bases, are a tool which is useful from both a computational-algorithmic perspective as well as from a theoretical perspective. We describe a Pommaret basis for the Veronese subrings $S^{(d)}$ given by $S^{(d)} = k[x^\mu \mid \deg x^\mu = d] \subseteq k[x_0,\ldots,x_n]$, i.e. a Pommaret basis of an ideal I where $S^{(d)} \cong R/I$ for the polynomial ring R in $\binom{n+d}{d}$ variables. From this construction, the theory of involutive bases immediately gives alternative proofs for some known properties of Veronese subrings as a corollary, such as their Castelnuovo-Mumford regularity and the fact that they are Cohen-Macaulay.

We combine the Pommaret basis with discrete algebraic Morse theory as presented in [1] to obtain a (non-minimal) free resolution. This construction enables us to give a formula for one non-vanishing Betti number of $S^{(d)}$ in each row of the Betti table. This result holds without any restriction on d. Our formula generalises a result from [2], where Ein and Lazarsfeld had given a similar statement, if d is sufficiently large. They conjectured that these Betti numbers are the first nonzero Betti numbers in each row. Additionally, our result has a relatively simple combinatorial interpretation: The non-vanishing statements for the Betti numbers in question translate to the existence of certain sets of multiindices of degree d.

References

[1] M. Albert, M. Fetzer, E. Sáenz-de-Cabezón and W. M. Seiler, *On the free resolution induced by a Pommaret basis*, J. Symbolic Comput. **68**, 2, pp. 4-26 (2015).

[2] L. Ein and R. Lazarsfeld, *Asymptotic syzygies of algebraic varietiese*, Invent. Math. **190**, 3, pp. 603-646 (2012).

Some computational elements of fractal topology based on HSF structures

C. Alemán, F. Cappelli, P. Real

H.S.T. Informatics Engineering, University of Sevilla (Spain) real@us.es

In [1], a kind of dense skeleton in terms of semi-directed graphs installed on the connectivity graph of fractal polyhedra, called Homological Spanning Forest (HSF, for short) is used for homotopically representing them. This research open a door to new topics within the areas of Fractal Topology [2] and Topological Recognition [3]. We here redesign the classical box-counting algorithm of fractal topology for digital images in terms of HSF notions and ideas.

References

[1] Molina-Abril, H., Real, P., Nakamura, A., Klette, R. (2015) *Connectivity calculus of fractal polyhedrons*. Pattern Recognition, **48(4)** 1150-1160.

[2] Porchon, H. (2012) *Fractal topology foundations*. Topology and its Applications, **159 (14)** 3156-3170.

[3] Laurentini A. (2001) *Topological recognition of polyhedral objects from multiples views*. Artificial Intelligence **v. 127(1)** 31-55.

An implementation of effective homotopy of fibrations [1]

A. Romero[1], J. Rubio[1], F. Sergeraert[2]

[1] *University of La Rioja, Spain, {ana.romero,julio.rubio}@unirioja.es*
[2] *Université Joseph Fourier,France, francis.sergeraert@ujf-grenoble.fr*

Abstract

In this paper, we present a new module for the Kenzo system which makes it possible to compute the effective homotopy of the total space of a fibration, using the well-known Serre exact sequence. The programs are written in Common Lisp and require the definition of new classes and functions and in particular include a new module for working with finitely generated Abelian groups. The chosen representation is that of a free presentation by means of a matrix in canonical form.

1 Introduction

Inspired by the fundamental ideas of the effective homology method (see [RS02]), in [RS12] a new *effective homotopy* theory was defined trying to allow the computation of *homotopy* groups of spaces. The most important notion is that of *a solution for the homotopical problem* of a Kan simplicial set, which consists of four algorithms describing in a *constructive* way the homotopy groups of a space, which is said to have *effective homotopy*. As in the case of effective homology, the idea consists in beginning by considering some spaces whose effective homotopy can be directly determined, and then different constructors of Algebraic Topology should produce new spaces with effective homotopy. As a first result in this research, in [RS12] we developed a theoretical algorithm to determine the effective homotopy of the total space of a fibration from the effective homotopies of the fiber and the base space.

In this work we present an implementation of the algorithm in [RS12] by means of a new module for the Kenzo system [DRSS99], consisting of about 4000 lines of Common Lisp code available at `http://www.unirioja.es/cu/anromero/research2.html`. In particular, it includes new structures and functions for working with finitely generated Abelian groups and computing kernels, cokernels and central extensions which are then used to implement the well-known Serre long exact sequence. The chosen representation for groups is that of a free presentation by means of a matrix in canonical form.

[1]This work has been partially supported by Ministerio de Economía y Competitividad, Spain, projects MTM2013-41775-P and MTM2014-54151.

2 A Kenzo module for finitely generated Abelian groups

As a necessary ingredient for the computation of the effective homotopy of the total space of a fibration, a new Kenzo module has been developed dealing with finitely generated Abelian groups. It consists of about 800 lines of code containing functions to construct groups and morphisms of groups and computing kernels, cokernels and central extensions. The chosen representation for groups is that of a free presentation by means of a matrix in *canonical form*. The reason why we prefer this representation to other options such as a list of divisors or a general matrix is to facilitate subsequent calculations.

Let G be a finitely generated Abelian group. The fundamental theorem of finitely generated Abelian groups asserts that G can be decomposed in a unique way as a direct sum of the form $\mathbb{Z}/\beta_1 \oplus \cdots \oplus \mathbb{Z}/\beta_r \oplus \mathbb{Z}^\alpha$ where each β_i divides β_{i+1}. This makes it possible to represent a group uniquely by means of a matrix $M_G : G_1 = \mathbb{Z}^r \to G_0 = \mathbb{Z}^{r+\alpha}$

$$M_G = \begin{bmatrix} \beta_1 & \cdots & 0 \\ & \ddots & \\ 0 & \cdots & \beta_r \\ 0 & \cdots & 0 \\ & \vdots & \\ 0 & \cdots & 0 \end{bmatrix} \tag{1}$$

where the number of rows with all entries equal to zero at the bottom of the matrix is given by α.

As said before, a group could also be represented by any general matrix, but the restriction of being a sparse matrix in canonical form is included to facilitate calculations on groups which will be necessary later. To this aim, a function called `canonical-representation` is provided computing the canonical form of a general matrix $N : N_1 \to N_0$ and returning a new matrix $N' : N'_1 \to N'_0$ as the one in (1). The canonical matrix N' is obtained by computing the Smith normal form of N and removing rows and lines corresponding to 1's and columns corresponding to 0's in the diagonal. The function also returns two matrices $R : N'_0 \to N_0$ and $R' : N_0 \to N'_0$ describing the relations between the original and the new generators (obtained also by means of the Smith normal form algorithm).

A morphism of finitely generated Abelian groups is then defined by means of two matrices which must commute with the matrices defining source and target groups. In this case the matrices can have as entries any integer number and no restriction is considered.

Let $f : A \to B$ be a morphism between two Abelian groups of finite type, given by matrices $M_0 : A_0 \to B_0$ and $M_1 : A_1 \to B_1$, and let us suppose that the groups A and B are represented respectively by matrices $M_A : A_1 \to A_0$ and $M_B : B_1 \to B_0$. The cokernel and kernel of f correspond respectively to the homology groups in degrees 0 and 1 of the bicomplex:

$$A_1 \overset{\begin{bmatrix} M_A \\ M_1 \end{bmatrix}}{\longrightarrow} A_0 \oplus B_1 \overset{\begin{bmatrix} M_0 & -M_B \end{bmatrix}}{\longrightarrow} B_0 \tag{2}$$

The cokernel is computed by considering the 1-degree differential matrix $[M_0 \ -M_B] \equiv D_1$ and computing its canonical form by means of our function `canonical-representation`. The new function `cokernel` inputs a morphism of finitely generated abelian groups $f : A \to B$ and returns a finitely generated abelian group C and a matrix $P : B_0 \to C_0$ where C_0 is the target of the matrix of the returned group C. The matrix P corresponds to the projection $B \to C = \text{Coker}$, which will be necessary later.

Similarly, the new function `kernel` inputs a morphism of finitely generated abelian groups $f : A \to B$ and returns a finitely generated abelian group K and a matrix $I : K_0 \to A_0$ where K_0 is the target of the matrix of the returned group K. The matrix I corresponds in this case to the inclusion $K = \ker \to A$ which will also be necessary later.

Let $0 \to A \to E \to C \to 1$ be a central extension of two finitely generated Abelian groups A and C. It is well-known (see [Bro82, Ch. VI.3]) there exists a set-theoretic map $\gamma : C \times C \to A$ which satisfies $\gamma(g,0) = 0 = \gamma(0,g)$ and $\gamma(g+h,k) = \gamma(h,k) - \gamma(g,h) + \gamma(g,h+k)$.

In addition, the initial extension is equivalent to another extension

$$0 \to A \to A \times_\gamma C \to C \to 1$$

where the elements of $A \times_\gamma C$ are pairs (a,c) with $a \in A$ and $c \in C$, and the group law is defined by

$$(a_1,c_1)(a_2,c_2) \equiv (a_1 + a_2 + \gamma(c_1,c_2), c_1 + c_2).$$

The set-theoretic map γ is called the 2-*cocycle* of the extension, since it corresponds to a map $\gamma : K(C,1)_2 \to A$ in the second group of cohomology $H^2(C,A)$, where $K(C,1)$ is an Eilenberg-MacLane space [May67, Ch.V].

Let us suppose that the groups A and C are represented respectively in Kenzo by means of the matrices $M_A : A_1 \to A_0$ and $M_C : C_1 \to C_0$. We consider a cocycle defined as a function $\gamma : C_0 \times C_0 \to A_0$. The central extension E is then defined by

means of a block matrix $M'_E : A_1 + C_1 \to A_0 + C_0$:

$$M'_E = \left[\begin{array}{c|c} M_A & M_\gamma \\ \hline 0 & M_C \end{array}\right] \tag{3}$$

The matrix M_γ is obtained as follows. For each g_i generator of C_1, we consider the element at the position (i,i) of the matrix M_C, d_i. The column i of the matrix M_γ is then defined by the element

$$M_\gamma(i) = -(\gamma(g_i, g_i) + \gamma(2 * g_i, g_i) + \cdots + \gamma((d_i - 1) * g_i, g_i))$$

The proof that the given matrix M'_E corresponds to a free presentation of the central extension $E \cong A \times_\gamma C$ can be found in `http://www.unirioja.es/cu/anromero/cer.pdf`.

But let us observe now that M'_E is not necessarily in canonical form and therefore it could not be used for our implementation of groups. To solve this problem, our function `canonical-representation` is applied to obtain the canonical form of the matrix M'_E, producing a new matrix $M_E : E_1 \to E_0$ which is valid for the definition. Our new Kenzo function `central-extension` returns the new group $E \cong A \times_\gamma C$ and two matrices $H : E_0 \to A_0 + C_0$ and $H' : A_0 + C_0 \to E_0$ which correspond to the relations between the generators of the final group E and the set $A_0 + C_0$.

3 Outcomes

Using the programs for working with finitely generated Abelian groups presented in the previous section, a new Kenzo module has been developed for the computation of the effective homotopy of the total space of a fibration. The implementation follows directly the proof presented in [RS12] (making use in particular of the Serre long exact sequence) and includes 4000 lines of code.

As an example of calculation of our programs, we consider the first steps of the Postnikov tower [May67, Ch.V] for the 2-sphere S^2. They can be built in Kenzo by means of the following statements:

```
>(progn
    (setf p2 (k-zp 0 2))
    (setf ch4 (chml-clss p2 4))
    (setf f3 (z-whitehead p2 ch4))
    (setf pfib3(twop-kanfibration f3))
    (setf p3 (sorc (fibr1 pfib3))))
[K735 Kan-Simplicial-Set-with-Effective-Homotopy]
```

The result is a Kan simplicial set with effective homotopy, stored in the variable p3, which corresponds to the total space of a fibration with twisting operator $f3 : K(\mathbb{Z},2) \to K(\mathbb{Z},3)$. The effective homotopy of this space is directly built by Kenzo from the effective homotopies of the base and the fiber, so that the homotopy groups of p3 can be determined. We can observe that they correspond to $\pi_i(S^2)$ for $i \leq 3$.

```
>(homotopy-group p3 1)
NIL
>(homotopy-group p3 2)
Component Z
>(homotopy-group p3 3)
Component Z
```

The process can be iterated and the space p_j of the tower satisfies $\pi_i(p_j) \cong \pi_i(S^2)$ for $i \leq j$. The following Kenzo code shows the result $\pi_6(S^2) \cong \mathbb{Z}/12$.

```
>(progn
  (setf ch5 (chml-clss p3 5))
  (setf f4 (zp-whitehead 2 p3 ch5))
  (setf pfib4 (twop-kanfibration f4))
  (setf p4 (sorc (fibr1 pfib4)))
  (setf ch6 (chml-clss p4 6))
  (setf f5 (zp-whitehead 2 p4 ch6))
  (setf pfib5 (twop-kanfibration f5))
  (setf p5 (sorc (fibr1 pfib5)))
  (setf ch7 (chml-clss p5 7))
  (setf f6 (zp-whitehead 12 p5 ch7))
  (setf pfib6 (twop-kanfibration f6))
  (setf p6 (sorc (fibr1 pfib6))))
 [K1430 Kan-Simplicial-Set-with-Effective-Homotopy]
>(homotopy-group p6 6)
Component Z/12Z
```

References

[Bro82] K. S. Brown. *Cohomology of Groups*. Springer-Verlag, 1982.

[DRSS99] X. Dousson, J. Rubio, F. Sergeraert, and Y. Siret. The Kenzo program. Institut Fourier, Grenoble, 1999. http://www-fourier.ujf-grenoble.fr/~sergerar/Kenzo/.

[May67] J. P. May. *Simplicial objects in Algebraic Topology*. Van Nostrand Mathematical Studies. University of Chicago Press, 1967.

[RS02] J. Rubio and F. Sergeraert. Constructive Algebraic Topology. *Bulletin des Sciences Mathématiques*, 126(5):389–412, 2002.

[RS12] A. Romero and F. Sergeraert. Effective homotopy of fibrations. *Applicable Algebra in Engineering, Communication and Computing*, 23:85–100, 2012.

Motion planning of robot arms with combinatorial restrictions

Jesús González[1], Bárbara Gutiérrez[2], and Sergey Yuzvinsky[3]

[1] *Cinvestav, México, jesus@math.cinvestav.mx*
[2] *Cinvestav, México, bgutierrez@math.cinvestav.mx*
[3] *University of Oregon, yuz@uoregon.edu*

We construct multitasking motion planners for automated systems whose space of states are homotopy equivalent to a polyhedral product space based on punctured spheres, e.g. robot arms with restrictions on the possible combinations of simultaneously moving nodes. Our construction is shown to be optimal by explicit cohomology calculations. The multitasking motion planning problem for other families of polyhedral product spaces is also determined.

Computing a new topological feature for grey-level 2D digital images: the topological hole tree

F. Díaz del Río (1), D. Onchis (2), P. Real (1)

(1) H.S.T. Informatics Engineering, University of Sevilla (Spain). fdiaz@atc.us.es, real@us.es
(2) Faculty of Mathematics, University of Vienna (Austria). darian.onchis@univie.ac.at

A computational framework for a new homotopy representation of a grey-level 2D digital image called *topological hole* tree is developed here. The computational advantages of this feature with regards to the well-known component tree structures (see, for example, [2, 3]) are showed in some applications like, for example, computing the RAG of a presegmented image or performing registration or retrieval. A parallel algorithm designed in [1] for computing HSF topological models is the core of the computation of the topological hole tree. Some experiments for understanding and extending the notion of topological hole tree to a 3D digital image are also given.

References

[1] Diaz-del-Rio, F., Real, P., Onchis, D (2015) *A parallel homological spanning forest framework for 2D topological image analysis*. Submitted to Pattern Recognition Letters, 2015.

[2] Petr Matas (2014) *Connected Component Tree Construction for Embedded Systems.* Ph.D. Thesis. University of West Bohemia.

[3] Caldairou, B., Naegel, B., Passat, N. (2009) *Segmentation of complex images based on component-trees: Methodological tools*. In Mathematical Morphology and Its Application to Signal and Image Processing (pp. 171-180). Springer Berlin Heidelberg.

S5
Difference Computer Algebra and its Applications

Bases for Modules of Difference-Operators by Gröbner Reduction

C. Fürst[1], G. Landsmann[1]

[1]*Johannes Kepler University Linz, Austria, Research Institute for Symbolic Computation (RISC)*

At the ISSAC 2015 conference, the authors have introduced the notion of **Gröbner Reduction** as an axiomatic approach to Gröbner bases techniques of filtered free modules [1]. Let R be a ring containing a field K, let F be a free R-module such that N is a submodule of F. The reduction relation $\longrightarrow$ is called a *Gröbner Reduction for N* provided that

1. $f \longrightarrow h \Rightarrow f \equiv h \pmod{N}$;
2. $\longrightarrow$ is a noetherian relation, i.e. every reduction sequence terminates in a finite number of steps;
3. The irreducible elements I in F build a monomial K-linear subspace, i.e. for all $f \in F$ we have $f \in I \Rightarrow \mathrm{supp}(f) \subseteq I$;
4. $I \cap N = 0$, i.e. every non-zero element is reducible;
5. For all $r \in \mathbf{N}^p$:
$$f \in F_r \wedge f \longrightarrow h \Rightarrow h \in F_r.$$

In that general setting, given a filtered module M_r (derived from a filtration R_r of the ring R), it is possible to compute the dimension of M_r viewn as K-vector space. In [2] it is shown that related ideas have been considered in literature for modules over non-commutative rings. The interplay of modules of this type (e.g. it is possible to model a differential ring by a particular Ore-algebra), confirm that a common theory might be applicable to modules over certain non-commutative rings. From that, it is possible to review

- **Reduction with Respect to Several Term Orderings** [3] for modules over the ring of Ore-polynomials;
- **Relative Reduction** [4] for modules over difference-differential rings;
- (x, ∂)**-Reduction** [5] for modules over Weyl-algebras,

under the aspect of Gröbner Reduction.

Recently, the authors have tried to view reduction in a more abstract setting. Precisely, if we have an ordered set $(Y,\leq)$ and an R-module M we consider a function $\mathrm{rk} : M \to Y$. We say that u reduces to v provided that

$$u \longrightarrow v :\Longleftrightarrow \exists g \in G \subseteq M\ \exists a \in A \subseteq R : v = u - ag \wedge \mathrm{rk}(v) < \mathrm{rk}(u). \qquad (1)$$

Let now $N := RG$. A reduction defined by the data (G,A,rk)

- is noetherian;
- satisfies $f \longrightarrow h \Rightarrow f \equiv h \pmod N$.

We can show, that under this assumptions the following holds.

Theorem. Let (G,A,rk) define the reduction relation (1). Then

- $I \cap N \subseteq 0 \Leftrightarrow N = Z$ where $Z := \{f \in N : f \longrightarrow^\star 0\}$;
- $M = N + I$;
- The irreducibles I build a monomial K-vector space.

In this talk, we want to report on research results that we are currently developing, and give an idea how the idea of Gröbner bases over modules can be unified in a way that a common theory applies for computation of (vector-space) dimension for filtered modules over filtered rings.

References

[1] C. Fürst and G. Landsmann, *Computation of Dimension in Filtered Free Modules by Gröbner Reduction*, Proceedings of the International Symposium on Symbolic and Algebraic Computation 2015, ACM (ed.), pp. 181-188. 2015

[2] C. Fürst and G. Landsmann, *Three Examples of Gröbner Reduction over Noncommutative Rings.*, Technical report no. 15-16 in RISC Report Series, Research Institute for Symbolic Computation (RISC), Johannes Kepler University Linz, Austria. October 2015

[3] A. Levin, *Gröbner bases with Respect to Several Term Orderings and Multivariate Dimension Polynomials*, Proceedings of the International Symposium on Symbolic and Algebraic Computation 2007, ACM (ed.), pp. 251-260. 2007

[4] F. Winkler and M. Zhou, *Computing difference-differential dimension polynomials by relative Gröbner bases in difference-differential modules*, Journal of Symbolic Computation, 43/10, 726-745, 2008.

[5] C. Dönch and A. Levin, *Computation of Bivariate Characteristic Polynomials of Finitely Generated Modules over Weyl Algebras*, International Journal of Algebra and Computation, 23, no. 7 (2013) , 1625 - 1651.

Difference algebra aided discretization of quasilinear evolution equations

V.P. Gerdt[1], Yu.A. Blinkov[2], K.B. Marinov[3]

[1] *Joint Institute for Nuclear Research, Dubna, Russia, gerdt@jinr.ru*
[2] *Saratov State University, Saratov, Russia, blinkovua@info.sgu.ru*
[3] *University "Dubna", Dubna, Russia, marinov.kohctahtih@gmail.com*

Let ∂_x be the derivation operator w.r.t. x and $\mathscr{R} := \mathbb{Q}(a_1,\ldots,a_i)\{u\}$ be the ordinary differential polynomial ring over the parametric field $\mathbb{Q}(a_1,\ldots,a_i)$ of constants. Here we consider a class of quasilinear evolution equations of the form

$$u_t = au_m + F(u_{m-1},\ldots,u_1,u)\,, \quad 0 \neq a \in \mathbb{Q}\,, \quad m \in \mathbb{N}_{>0}\,, \tag{1}$$

where $u_k := \partial_x^k u$ $(0 \leq k \leq m)$, $u_0 := u$ and $F \in R$ is a differential polynomial of the order $m-1$ in ∂_x (denotation: $\mathrm{ord}(F) = m-1$) such that there is a differential polynomial $P \in \mathscr{R}$ satisfying

$$F = \partial_x P = \sum_{k=0}^{m-2} u_{k+1}\frac{\partial P}{\partial u_k}\,. \tag{2}$$

Given F, one can algorithmically verify whether or not such P exists and construct it in the case of existence. The equality (2) means that (1) admits the conservation law form

$$u_t = \partial_x\left(au_{m-1} + P\right)\,, \quad P \in \mathscr{R}\,, \quad \mathrm{ord}(P) = m-2\,. \tag{3}$$

The set of evolution equations admitting the polynomial conservation law (3) contains most of classical evolution equations, e.g., the Korteveg-de Vries (KdV) equation and KdV hierarchy, the Burgers equation and Burgers hierarchy, the Kuramoto-Sivashinsky equation, the Burgers-Huxley equation, etc., and their various generalizations (cf. [1]). All these equations have exact solutions that are useful in analysis of numerical methods for their solving.

To discretize equation (3), we follow the approach of paper [2] and convert the equation into the equivalent integral form

$$\oint_\Gamma (P + au_{m-1})\,dt + u\,dx = 0\,, \tag{4}$$

where Γ is an arbitrary singly connected integration contour. Using the standard notation $u_j^n = u(t_n, x_j)$ for the grid function and the Cartesian grid with $t_{n+1} - t_n = \tau$, $x_{j+1} - x_j = h$ we choose the rectangular integration contour as a "control volume" (cf. [2]) and add $m-2$ integral relations

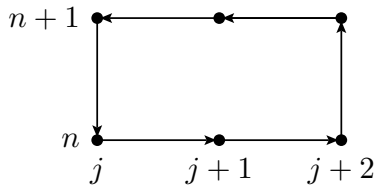


Figure 1: Basic integration contour

$$\int_{x_j}^{x_{j+1}} u_{k+1}\,dx = u_k(t,x_{j+1}) - u_k(t,x_j)\,, \quad k = 1,\ldots,m-2\,. \tag{5}$$

Now, to discretize (4) we apply a numerical evaluation method to the contour integral (4) in order to express it in terms of the grid functions and also (possibly different) numerical evaluation methods to the integrals in the left-hand sides of (5). Thereby, we obtain a system of difference equations containing $u_j^n, {u_1}_j^n, \ldots, {u_{m-1}}_j^n$. The last step in generation of a finite difference approximation (FDA) to (1) is algebraic elimination of the grid functions ${u_1}_j^n, \ldots, {u_{m-1}}_j^n$, which correspond to the proper partial derivatives of u, from the discrete system obtained. Such elimination can be done by means of the MAPLE package *LDA* [3] which is freely available (`http://wwwb.math.rwth-aachen.de/Janet/`).

We illustrate the above described approach by example of the KdV equation

$$u_t + u_{xxx} + 6uu_x = 0\,. \tag{6}$$

Its integral conservation law form for the contour Γ of Figure 1 reads

$$\oint_{\mathscr{C}} (u_{xx} + 3u^2)\,dt + u\,dx = 0\,. \tag{7}$$

To approximate numerically the contour integral, we apply the trapezoidal rule to the integration over t as well as to the integration over x. For numerical approximations of the integral relations we apply the trapezoidal rule for the integration of u_x and the midpoint rule for the integration of u_{xx}. This leads to the difference approximation to (6) which is outputted by the following MAPLE code shown in Figure 2 with $P := 3u^2$. The output is the left-hand side of the FDA to (6) written in the conventional form as

$$\frac{u_j^{n+1} - u_j^n}{\tau} + \frac{(P_{j+1}^{n+1} - P_{j-1}^{n+1}) + (P_{j+1}^n - P_{j-1}^n)}{4h} + \\ + \frac{(u_{j+2}^{n+1} - 2u_{j+1}^{n+1} + 2u_{j-1}^{n+1} - u_{j-2}^{n+1}) + (u_{j+2}^n - 2u_{j+1}^n + 2u_{j-1}^n - u_{j-2}^n)}{4h^3} = 0\,.$$

```
> with(LDA):
> L:=[(-(P(n,j)+P(n+1,j)-P(n,j+2)-P(n+1,j+2)) -
      (uxx(n,j)+uxx(n+1,j)-uxx(n,j+2)-uxx(n+1,j+2)))*tau/2+
      (u(n+1,j+1)-u(n,j+1))*2*h,
     (ux(n,j+1)+ux(n,j))*h/2-(u(n,j+1)-u(n,j)),
      2*uxx(n,j+1)*h-(ux(n,j+2)-ux(n,j))];
```

$$L := \left[\frac{1}{2}\,(-P(n,j) - P(n+1,j) + P(n,j+2) + P(n+1,j+2) - uxx(n,j) - uxx(n+1,j) + uxx(n,j \tag{1}$$

$$+ 2) + uxx(n+1,j+2))\,\tau + 2\,(u(n+1,j+1) - u(n,j+1))\,h,\ \frac{1}{2}\,(ux(n,j+1) + ux(n,j))\,h$$

$$- u(n,j+1) + u(n,j),\ 2\,uxx(n,j+1)\,h - ux(n,j+2) + ux(n,j)\Big]$$

```
> JanetBasis(L,[n,j],[uxx,ux,u,F],2):
> collect(%[1,1]/(4*tau*h**3),[tau,h]);
```

$$\frac{\frac{1}{4}P(n+1,j+3) + \frac{1}{4}P(n,j+3) - \frac{1}{4}P(n+1,j+1) - \frac{1}{4}P(n,j+1)}{h} + \frac{1}{h^3}\left(\frac{1}{4}u(n+1,j+4)\right. \tag{2}$$

$$- \frac{1}{2}u(n+1,j+3) + \frac{1}{4}u(n,j+4) - \frac{1}{2}u(n,j+3) + \frac{1}{2}u(n+1,j+1) - \frac{1}{4}u(n+1,j)$$

$$\left. + \frac{1}{2}u(n,j+1) - \frac{1}{4}u(n,j)\right) + \frac{u(n+1,j+2) - u(n,j+2)}{\tau}$$

Figure 2: Construction of FDA to KdV with MAPLE

Since the obtained FDA to (6) has quadratic nonlinearity (due to $P = 3u^2$) in the grid function on the next time layer, in order to construct a numerical solution we use the following approximate linearization

$$v_{k+1}^2 = v_{k+1}^2 - v_k^2 + v_k^2 = (v_{k+1} - v_k)(v_{k+1} + v_k) + v_k^2 \approx v_{k+1} \cdot 2v_k - v_k^2 .$$

By taking this linearization into account, we implemented a numerical procedure for construction of a solution to KdV in Python 2.7 freely downloadable from the Web page `https://www.python.org/download/releases/2.7/`. Figure 3 demonstrates the time evolution of numerical solution in the domain $x \in [0,200]$ with $h = 0.4$ and $\tau = 0.2$ and for the initial value (Cauchy) problem with the initial data

$$u(t=0) := f(x,0,0.4) + f(x-20,0,0.2)$$

where

$$f(x,t,\kappa) := \frac{2\kappa^2}{\cosh^2\left[\kappa(x - 4\kappa^2 t)\right]}$$

is the exact one-soliton solution to (6). As Figure 3 shows, the constructed numerical solution reveals a behavior inherent to localized solutions of KdV.

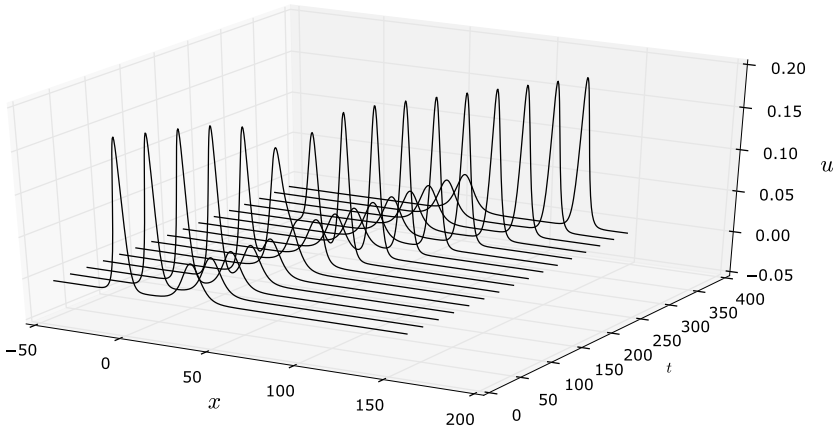


Figure 3: Dynamics of solution to KdV

References

[1] N.A.Kudryashov. Methods of Nonlinear Mathematical Physics. Publishing House “Intellect”, 2010 (in Russian).

[2] V. P. Gerdt, Yu. A. Blinkov, and V. V. Mozzhilkin. Gröbner Bases and Generation of Difference Schemes for Partial Differential Equations. *Symmetry, Integrability and Geometry: Methods and Applications*, 2:051, 2006, 26 pages. arXiv:mathRA/0605334

[3] V. P. Gerdt and D. Robertz. A Maple Package for Computing Gröbner Bases for Linear Recurrence Relations. *Nuclear Instruments and Methods in Physics Research*, A559:215–219, 2006. arXiv:cs.SC/0509070.

Difference Dimension Quasi-polynomials

Alexander Levin

The Catholic University of America, USA, levin@cua.edu

Let K be a (not necessarily inversive) difference field of zero characteristic with basic set of translations $\sigma = \{\alpha_1, \ldots, \alpha_m\}$ that are assigned rational weights $w_1, \ldots, w_m$, respectively. Let T denote the free commutative semigroup generated by σ and for any transform $\tau = \alpha_1^{k_1} \ldots \alpha_m^{k_m} \in T$, let

$$\mathrm{ord}_w \tau = \sum_{i=1}^{m} w_i k_i.$$

Furthermore, for any $r \in \mathbb{N}$, let $T_w(r) = \{\tau \in T \mid \mathrm{ord}_w \tau \leq r\}$.

In this talk we present the following result.

Theorem. *With the above notation, let $L = K\langle \eta_1, \ldots, \eta_n \rangle$ be a difference field extension of K generated by a finite set $\eta = \{\eta_1, \ldots, \eta_n\}$ and for any $r \in \mathbb{N}$, let $L_r = K(\cup_{i=1}^{n} T_w(r)\eta_i)$. Then there exists a quasi-polynomial $\Phi_{\eta|K}(t)$ such that*

(i) *$\Phi_{\eta|K}(r) = \mathrm{tr.deg}_K L_r$ for all sufficiently large $r \in \mathbb{N}$.*

(ii) *$\deg \Phi_{\eta|K} \leq m$.*

(iii) *$\Phi_{\eta|K}$ is an alternative sum of Ehrhart quasi-polynomials associated with rational conic polytopes. The leading coefficient of the quasi-polynomial $\Phi_{\eta|K}$ is a constant that does not depend on the set of difference generators η of the extension L/K. Furthermore, the coefficient of t^m in $\Phi_{\eta|K}$ is equal to the difference transcendence degree of L/K.*

This theorem generalizes the corresponding result on difference dimension polynomials introduced in [3] (see also [4] where properties and applications of difference dimension polynomials are discussed). The quasi-polynomial $\Phi_{\eta|K}$ is called the *difference dimension quasi-polynomial* associated with the extension L/K and the system of difference generators η.

Note that the existence of Ehrhart-type dimension quasi-polynomials associated with weighted filtrations of differential and inversive difference modules was established by C. Dönch in his dissertation [1]. C. Dönch also proved the existence of dimension quasi-polynomials associated with finitely generated differential and inversive difference field extensions (see [1, Theorem 3.1.13]) using the

technique of weight Gröbner bases in the associated modules of Kähler differentials. This method, however, cannot be applied to a non-inversive difference field extension, since in this case there is no natural difference module structure of the corresponding module of Kähler differentials. In order to prove the above theorem, we apply the technique of characteristic sets (with respect to a ranking that respects the weighted order of transforms) and the following proposition that generalizes Kolchin's result on dimension polynomials of subsets of $\mathbb{N}^m$ (see [2, Chapter 0, Lemma 16]).

Let $\leq_P$ denote the product order on $\mathbb{N}^m$ ($m \in \mathbb{N}$, $m \geq 1$), that is a partial order such that $(a_1, \ldots, a_m) \leq_P (b_1, \ldots, b_m)$ if and only if $a_i \leq b_i$ for $i = 1, \ldots, m$. Let $w_1, \ldots, w_m$ be fixed non-negative rational numbers and for any $a = (a_1, \ldots, a_m) \in \mathbb{N}^m$, let $\operatorname{ord}_w a = w_1 a_1 + \cdots + w_m a_m$.

If $A \subseteq \mathbb{N}^m$ and $r \in \mathbb{N}$, then $A(r)$ will denote the set of all $a = (a_1, \ldots, a_m) \in A$ such that $a_1 + \cdots + a_m \leq r$. Furthermore, if $A \subseteq \mathbb{N}^m$, then V_A will denote the set of all m-tuples $v = (v_1, \ldots, v_m) \in \mathbb{N}^m$ that are not greater than or equal to any m-tuple from A with respect to $\leq_P$. (Clearly, an element $v = (v_1, \ldots, v_m) \in \mathbb{N}^m$ belongs to V_A if and only if for any element $(a_1, \ldots, a_m) \in A$ there exists $i \in \mathbb{N}, 1 \leq i \leq m$, such that $a_i > v_i$.)

Proposition. *With the above conventions, for any set $A \subseteq \mathbb{N}^m$, there exists a quasi-polynomial $\omega_A(t)$ in one variable t such that*

(i) $\omega_A(r) = \operatorname{Card} V_A(r)$ *for all sufficiently large* $r \in \mathbb{N}$.

(ii) $\deg \omega_A \leq m$.

(iii) $\deg \omega_A = m$ *if and only if* $A = \emptyset$.

(iv) $\omega_A = 0$ *if and only if* $(0, \ldots, 0) \in A$.

With the notation of the theorem, one can use the above proposition to express the quasi-polynomial $\Phi_{\eta|K}(t)$ as an alternative sum of quasi-polynomials of the form $\omega_A(t)$ where $A \subseteq \mathbb{N}^m$. It allows one to obtain methods of computation of difference dimension quasi-polynomials based on known algorithms for computing Ehrhart quasi-polynomials of rational polytopes. We will give some corresponding examples and discuss an interpretation of a difference dimension quasi-polynomial as the strength of a system of difference equations with weighted translations. Such systems arise, in particular, from finite difference approximations of systems of PDEs with weighted derivations (see, for example, [5] and [6]).

References

[1] C. Dönch, *Standard Bases in Finitely Generated Difference-Skew-Differential Modules and Their Application to Dimension Polynomials*, Ph. D. Thesis, Johannes Kepler University Linz, Research Institute for Symbolic Computation (RISC), 2012.

[2] E. R. Kolchin. *Differential Algebra and Algebraic Groups*. Academic Press, 1973.

[3] A. B. Levin. *Characteristic polynomials of filtered difference modules and of difference field extensions*. Russian Math. Surveys, 33 (1978), no. 3, 165-166.

[4] A. B. Levin. *Difference Algebra*. Springer, 2008.

[5] N. A. Shananin. *Partial quasianalyticity of distribution solutions of weakly nonlinear differential equations with weights assigned to derivatives*. Math. Notes, 68 (2000), no. 3–4, 519–527.

[6] N. A. Shananin. *Propagation of the invariance of germs of solutions of weakly nonlinear differential equations with weighted derivatives*. Math. Notes, 71 (2002), no. 1–2, 123–130.

Gröbner basis driven construction of a new s-consistent difference approximation to Navier-Stokes equations

P. Amodio[1], Yu.A. Blinkov[2], V.P. Gerdt[3], R. La Scala[1]

[1] *University of Bari, Bari, Italy, {pierluigi.amodio, roberto.lascala}@uniba.it*
[2] *Saratov State University, Saratov, Russia, blinkovua@info.sgu.ru*
[3] *Joint Institute for Nuclear Research, Dubna, Russia, gerdt@jinr.ru*

The quality of a numerical solution to a partial differential equation (PDE) or to a system of PDEs obtained by the finite difference method is determined by the underlying finite difference approximation (FDA) to the PDE(s). It is a challenging problem to construct a FDA which inherits or mimics at the discrete level the fundamental properties of the original PDE(s) such as topology, symmetries, conservation laws, maximum principle, etc. Such FDAs are called *compatible* or *mimetic* (cf. [2]).

In [7], for linear PDE systems and regular (Cartesian) grids, the necessary condition for compatibility of FDA, *s(strong)-consistency*, was established. This condition admits an algorithmic verification via difference Gröbner bases. It was generalized in [3, 6, 8] to polynomially-nonlinear systems of PDEs.

Let F be a finite set of differential polynomials, $\{f = 0 \mid f \in F\}$ be the corresponding PDE system, $\tilde{F}$ be the set of difference polynomials such that set $\{\tilde{f} = 0 \mid \tilde{f} \in \tilde{F}\}$ forms a FDA to the PDE system on a chosen (regular) solution grid. Then FDA is called s-consistent if

$$(\forall \tilde{g} \in [\![\tilde{F}]\!])\ (\exists g \in [\![F]\!])\ [\tilde{g} \text{ is FDA to } g]$$

where $[\![\tilde{F}]\!]$ and $[\![F]\!]$ is respectively the perfect difference ideal (cf. [9]) generated by $\tilde{F}$ and the perfect differential ideal generated by $\tilde{F}$.

By applying the approach of paper [5] to the two-dimensional Navier-Stokes equations describing the unsteady motion of an incompressible viscous liquid of constant viscosity

$$\begin{cases} f_1 := & u_x + v_y = 0\,, \\ f_2 := & u_t + uu_x + vu_y + p_x - \frac{1}{\mathrm{Re}}\Delta u = 0\,, \\ f_3 := & v_t + uv_x + vv_y + p_y - \frac{1}{\mathrm{Re}}\Delta v = 0\,. \end{cases} \tag{1}$$

where (u,v) is the velocity field, p is the pressure, the constant Re is the Reynolds number, we constructed in [4] two s-consistent FDAs to (1). Below we refer to these FDAs as to FDA2 and FDA3. In [1] we showed the numerical superiority

of FDA2 over two other FDAs that are not s-consistent. In doing so, we used the exact solution [10] to (1)

$$u = -e^{-\frac{2t}{\mathrm{Re}}}\cos(x)\sin(y),\ v = e^{-\frac{2t}{\mathrm{Re}}}\sin(x)\cos(y),\ p = -\frac{1}{4}e^{-\frac{4t}{\mathrm{Re}}}(\cos(2x)+\cos(2y)). \quad (2)$$

and the grid with temporal spacing τ and the spatial spacing h for both x and y.

In this talk we propose a new FDA that we obtained in the following way. We have started with a direct difference approximation of the single equations (1). In the conventional notations

$$u^n_{j,k} := u(n\tau, xj, yk), \quad v^n_{j,k} := v(n\tau, xj, yk), \quad p^n_{j,k} := p(n\tau, xj, yk)$$

for the grid functions u, v, p such approximation reads

$$\begin{aligned}
&\frac{u^n_{j+1,k}-u^n_{j-1,k}}{2h}+\frac{v^n_{j,k+1}-v^n_{j,k-1}}{2h}=0,\\
&\frac{u^{n+1}_{j,k}-u^n_{j,k}}{\tau}+\frac{(u^n_{j+1,k})^2-(u^n_{j-1,k})^2}{2h}+\frac{v^n_{j,k+1}u^n_{j,k+1}-v^n_{j,k-1}u^n_{j,k-1}}{2h}+\frac{p^n_{j+1,k}-p^n_{j-1,k}}{2h}\\
&\qquad -\frac{1}{\mathrm{Re}}\left(\frac{u^n_{j+1,k}-2u^n_{j,k}+u^n_{j-1,k}}{h^2}+\frac{u^n_{j,k+1}-2u^n_{j,k}+u^n_{j,k-1}}{h^2}\right)=0, \quad (3)\\
&\frac{v^{n+1}_{j,k}-v^n_{j,k}}{\tau}+\frac{(v^n_{j,k+1})^2-(v^n_{j,k-1})^2}{2h}+\frac{u^n_{j+1,k}v^n_{j+1,k}-u^n_{j-1,k}v^n_{j-1,k}}{2h}+\frac{p^n_{j,k+1}-p^n_{j,k-1}}{2h}\\
&\qquad -\frac{1}{\mathrm{Re}}\left(\frac{v^n_{j+1,k}-2v^n_{j,k}+v^n_{j-1,k}}{h^2}+\frac{v^n_{j,k+1}-2v^n_{j,k}+v^n_{j,k-1}}{h^2}\right)=0.
\end{aligned}$$

Aiming to obtain a time-independent equation with linear leading monomial in the variable p in order to solve numerically the FDA, we have performed a difference Gröbner basis computation with pure lexicographic ordering with $p > u > v$ and $\partial_t > \partial_x > \partial_y$. We have obtained then a finite difference Gröbner basis consisting of 5 elements where we have found an equation of the required form, namely

$$\begin{aligned}
&\frac{p^n_{j+2,k}-2p^n_{j,k}+p^n_{j-2,k}}{4h^2}+\frac{p^n_{j,k+2}-2p^n_{j,k}+p^n_{j,k-2}}{4h^2}\\
&\quad+\frac{(u^n_{j+2,k})^2-2(u^n_{j,k})^2+(u^n_{j-2,k})^2}{4h^2}+\frac{(v^n_{j,k+2})^2-2(v^n_{j,k})^2+(v^n_{j,k-2})^2}{4h^2}\\
&\quad+2\frac{u^n_{j+1,k+1}v^n_{j+1,k+1}-u^n_{j+1,k-1}v^n_{j+1,k-1}-u^n_{j-1,k+1}v^n_{j-1,k+1}+u^n_{j-1,k-1}v^n_{j-1,k-1}}{4h^2} \quad (4)\\
&\quad+\frac{2}{\mathrm{Re}}\frac{-u^n_{j+2,k}+4u^n_{j+1,k}-4u^n_{j-1,k}+u^n_{j-2,k}-u^n_{j+1,k+1}-u^n_{j+1,k-1}+u^n_{j-1,k+1}+u^n_{j-1,k-1}}{4h^3}\\
&\quad+\frac{2}{\mathrm{Re}}\frac{-v^n_{j,k+2}+4v^n_{j,k+1}-4v^n_{j,k-1}+v^n_{j,k-2}-v^n_{j+1,k+1}-v^n_{j-1,k+1}+v^n_{j+1,k-1}+v^n_{j-1,k-1}}{4h^3}=0.
\end{aligned}$$

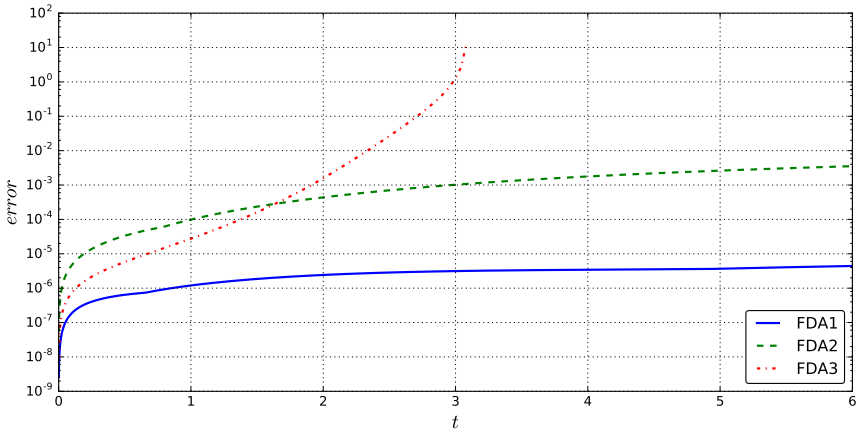


Figure 1: Dynamics of numerical error

It is interesting to note that this computer-generated difference equation is in fact the approximation of the following differential equation

$$(p_{xx}+p_{yy})+2(u_x^2+u_xv_y+u_yv_x+v_y^2+u(u_{xx}+v_{xy})+v(u_{xy}+v_{yy}))+ \\ -\frac{1}{\mathrm{Re}}(u_{xxx}+u_{xyy}+v_{xxy}+6v_{yyy})=0.$$

One can check that this equation belongs to the differential ideal generated by the Navier-Stokes equations (1) which provides the s-consistency of a new scheme FDA1 that we have obtained by joining the equation (4) to the difference system (3).

Figure 1 demonstrates dynamics of the numerical errors in computation of pressure p for the three difference approximations, FDA1 and two s-consistent FDAs (FDA2 and FDA3) constructed in [4], and for the Cauchy problem with initial data taken according to (2). As one can see from the figure, the numerical behavior of FDA1 is much better than that of FDA2 and FDA3. In doing so, FDA3 reveals instability. The errors in u and v have similar behavior.

References

[1] P. Amodio, Yu.A. Blinkov, V. P. Gerdt, R. La Scala. On Consistency of Finite Difference Approximations to the Navier-Stokes Equations. *Computer Algebra in Scientific Computing / CASC 2013*, V. P. Gerdt, W. Koepf, E. W. Mayr, E. V. Vorozhtsov (Eds.), LNCS 8136, pp. 46–60. Springer, Cham, 2013. arXiv:math.NA/1307.0914

[2] D. N. Arnold, P. B. Bochev, R.B. Lehoucq, R. A.Nicolaides, M. Shashkov (Eds.) Compatible Spatial Discretizations. *The IMA Volumes in Mathematics and its Applications*, Vol. 142. Springer, 2006.

[3] V. P. Gerdt. Consistency Analysis of Finite Difference Approximations to PDE Systems. Mathematical *Modelling in Computational Physics / MMCP 2011*, Adam, G., Buša, J., Hnatič, M. (Eds.), LNCS 7125, pp. 28–42. Springer, Berlin (2012). arXiv:math.AP/1107.4269

[4] V. P. Gerdt, Yu.A. Blinkov. Involution and Difference Schemes for the Navier-Stokes Equations. *Computer Algebra in Scientific Computing / CASC 2009*, V. P. Gerdt, E. W. Mayr, E. V. Vorozhtsov (Eds.), LNCS 5743, pp. 94–105. Springer, Berlin, 2009.

[5] V. P. Gerdt, Yu. A. Blinkov, V. V. Mozzhilkin. Gröbner Bases and Generation of Difference Schemes for Partial Differential Equations. *Symmetry, Integrability and Geometry: Methods and Applications*, 2:26, 2006.

[6] V. P. Gerdt, R. La Scala, Noetherian quotients of the algebra of partial difference polynomials and Gröbner bases of symmetric ideals, *Journal of Algebra*, 423, 1233–1261, 2015.

[7] V. P. Gerdt, D. Robertz. Consistency of Finite Difference Approximations for Linear PDE Systems and its Algorithmic Verification). Watt, S.M. (Ed.), *Proceedings of ISSAC 2010*, pp. 53–59. Association for Computing Machinery (2010).

[8] R. La Scala, Gröbner bases and gradings for partial difference ideals, *Math. Comp.*, 84, 959–985, 2015.

[9] A. Levin. Difference Algebra. *Algebra and Applications*, Vol. 8. Springer, 2008.

[10] J. Kim, P. Moin. Application of a Fractional-Step Method To Imcompressible Navier-Stokes Equations. *J. Comput. Phys.* 59, 308–323, 1985.

Binomial partial difference ideals

C.M. Yuan[1]

[1] *Academy of systems science, CAS, China, {cmyuan}@mmrc.iss.ac.cn*

In [1], we present some basic concepts and properties of binomial difference ideals. A natural question is that what about the partial difference case? The main difference between the ordinary difference case and the partial difference case is that in partial difference case, the difference operators may have relations and the algorithms for the ordinary difference case can not be used directly.

Let F be a partial difference field, and $\sigma_1,\ldots,\sigma_m$ be m partial difference operators. F is said to be *inversive* if for any i such that $\sigma_i a \in F$ implies $a \in F$. Let Θ be the multiplicative closed set with unit of these m partial difference operators. Let $Y=\{y_1,\ldots,y_n\}$ be n difference indeterminates. Then, the elements of $F\{Y\}=F[\Theta y_j^{\cdot} j=1,\ldots,n]$ are called *partial difference polynomials* over F in Y, and $F\{Y\}$ itself is called the *partial difference polynomial ring* over F in Y. A *partial difference polynomial ideal* I in $F\{Y\}$ is an ordinary algebraic ideal which is closed under transforming, i.e. $\sigma_i(I)\subset I$ for any i. If I also has the property that for any $1\leq i\leq m$, $\sigma_i a\in I$ implies that $a\in\mathscr{I}$, it is called a *reflexive partial difference ideal*. And a prime partial difference ideal is a partial difference ideal which is prime as an ordinary algebraic polynomial ideal.

Since if F is not algebraically closed, Bentsen [2] show that one irreducible polynomial may has no solution in its extension field. In order to avoid this, F is assumed to be algebraically closed, inversive and of characteristic zero. We introduce the following useful notation. Let $x_1,\ldots,x_m$ be m algebraic indeterminates and $p=\sum c_{k_1,\ldots,k_m}\prod_{i=1}^m x_i^{k_i}\in\mathbf{Z}[x_1,\ldots,x_m]$. For a in any over field of F, denote

$$a^p=\prod(\sigma_i^{k_i}a)^{c_{k_1,\ldots,k_m}}.$$

For instance, if $m=2$, then $a^{x_1^2+2x_2-1}=(\sigma_1^2 a)(\sigma_2 a)^2/a$. It is easy to check that for $p,q\in\mathbf{Z}[x_1,\ldots,x_m]$, and a,b in any over field of F, we have

$$a^{p+q}=a^p a^q, a^{pq}=(a^p)^q, (ab)^p=a^p b^p. \tag{1}$$

For $\mathbf{f}=(f_1,\ldots,f_n)^\tau\in\mathbf{Z}[x_1,\ldots,x_m]^n$, we define $Y^{\mathbf{f}}=\prod_{i=1}^n y_i^{f_i}$. $Y^{\mathbf{f}}$ is called a *Laurent partial difference monomial* in Y and $\mathbf{f}$ is called its *support*.

A *Laurent partial difference polynomial* over F in Y is an F-linear combination of Laurent partial difference monomials in Y. Clearly, the set of all Laurent partial difference polynomials form a commutative partial difference ring under the obvious sum, product, and the partial difference operators σ_i, where all Laurent

partial difference monomials are invertible. We denote the partial difference ring of Laurent partial difference polynomials with coefficients in F by $F\{Y^{\pm}\}$.

A polynomial ideal I is called binomial if it is generated by polynomials with at most two terms. By a *Laurent partial difference binomial* in Y, we mean a partial difference polynomial with two terms, that is, $aY^{\mathbf{f}_1} + bY^{\mathbf{f}_2}$ where $a, b \in F^* = F \setminus \{0\}$ and $\mathbf{f}_1, \mathbf{f}_2 \in \mathbf{Z}[x_1, \ldots, x_m]^n$. A Laurent partial difference binomial of the following form is said to be in *normal form*

$$p = Y^{\mathbf{f}} - c_{\mathbf{f}} \tag{2}$$

A Laurent partial difference ideal is called binomial if it is generated by Laurent partial difference binomials. Then, we have

Lemma 1 *Let I be a Laurent binomial partial difference ideal and*

$$L(I) := \{\mathbf{f} \in \mathbf{Z}[x_1, \ldots, x_m]^n \mid \exists c_{\mathbf{f}} \in F^* \, s.t. \, Y^{\mathbf{f}} - c_{\mathbf{f}} \in I\}. \tag{3}$$

Then $L(I)$ is a $\mathbf{Z}[x_1, \ldots, x_m]$ modular, which is called the support modular *of I.*

This lemma means that the properties of a Laurent binomial partial difference ideal is related to its support modular.

Based on this lemma and the partial characteristic set method [3], we may decompose the zero set of a Laurent binomial partial difference ideal I into a set of prime ideals with their characteristic set are strong irreducible. Moreover, let $\mathbf{m}$ be the monomial set in $x_1, \ldots, x_m$, if we denote by $L_S = \{\mathbf{f} \in \mathbf{Z}[x_1, \ldots, x_m]^n | \exists c \in \mathbf{Z}, \mathbf{g} \in \mathbf{m}, s.t. cg \in L\}$.

Theorem 1 *Let I be a Laurent binomial partial difference ideal, L its support modular, and L_S the saturation of L. Then $\{I\}$ is either $[1]$ or can be written as the intersection of Laurent reflexive prime binomial partial difference ideals whose support modular is L_S.*

Definition 1 *Let L be a $\mathbf{Z}[x_1, \ldots, x_m]$-module in $\mathbf{Z}[x_1, \ldots, x_m]^n$.*

- *L is called* $\mathbf{Z}$-saturated *if, for any $a \in \mathbf{Z}$ and $\mathbf{f} \in \mathbf{Z}[x_1, \ldots, x_m]^n$, $a\mathbf{f} \in L$ implies $\mathbf{f} \in L$.*
- *L is called* x-saturated *if, for any $\mathbf{f} \in \mathbf{Z}[x_1, \ldots, x_m]^n$, $x_i\mathbf{f} \in L$ implies $\mathbf{f} \in L$ for any i.*
- *L is called* saturated *if it is both $\mathbf{Z}$- and x- saturated.*

Then, we have the following result

Theorem 2 *If F is algebraically closed and inversive, I is a non-trivial Laurent binomial partial difference ideal and L its support modular, then*

(a) *L is $\mathbf{Z}$-saturated if and only if I is prime;*

(b) *L is x-saturated if and only if I is reflexive;*

(c) *L is saturated if and only if I is reflexive prime.*

Also, we have algorithms to check whether a given $\mathbf{Z}[x_1,\ldots,x_m]$ modular L is $\mathbf{Z}$-saturated(x-saturated) or not, and in the negative case, to compute the $\mathbf{Z}$-saturation(x-saturation) of L.

Using these algorithms, we can decompose the zero set of a binomial partial difference ideal I into the union of the zero set of reflexive prime binomial partial difference ideals.

References

[1] X.S. Gao, Z. Huang, C.M. Yuan, *Binomial Difference Ideals*, arXiv:1603.03987, (2016).

[2] I. Bentsen, *The Existence of Solutions of Abstract Partial Difference Polynomials*, Trans- actions of the Amer. Math. Soc., 158, 373-397(1972).

[3] G.L. Zhang, X.S. Gao, *Properties of Ascending Chians fr Partial Difference Polynomial Systems*, LNAI 5081, 307-321 (2008).

Order Bounds for a Difference Decomposition Algorithm

E. Amzallag[1], R. Gustavson[2],

[1] *CUNY Graduate Center, New York, NY, eamzallag@gradcenter.cuny.edu*
[2] *CUNY Graduate Center, New York, NY, rgustavson@gradcenter.cuny.edu*

Given a system of polynomial difference equations $F = 0, F = f_1, \ldots, f_r$, it is often difficult to determine if the system has a solution, let alone what the solutions are. Difference algebraically, this problem becomes one of determining membership in the perfect difference ideal generated by F. A membership test for the perfect difference ideal generated by a finite collection of difference polynomials can also be used to test for difference algebraic dependencies of other difference polynomials. It is thus essential to have algorithmic methods for determining membership in a perfect difference ideal, and to have complexity estimates for them.

An algorithm to solve this problem was developed in [1]. Given a finite system of difference polynomials over the field of rational functions with automorphism mapping $f(x) \in \mathbb{Q}(x)$ to $f(x+1) \in \mathbb{Q}(x)$, the algorithm ultimately produces what the authors call a Ritt-Wu decomposition of the zero set of the given system. The authors show that this algorithm will either output a useful decomposition of the zero set to solve the system or indicate that the system has no solution. This then, in addition, allows us to test for membership in the perfect difference ideal generated by a finite collection of difference polynomials.

For a complexity bound on this algorithm, we seek a bound on the orders of the difference polynomials produced at each step of the algorithm in terms of the original system. One of the key steps of the algorithm involves the computation of difference ascending chains associated to the given collection of difference polynomials. In this talk, we will present the first known theoretical upper bound for the orders of the ascending chains produced in this algorithm. The bound depends on the number of difference variables, the order and degree of the original system, and the number of elements in the original system. We achieved this bound by proving an effective version of the well-known result by Ritt and Doob which showed that every strictly decreasing sequence of difference ascending chains is finite.

References

[1] X.-S. Gao, Y. Luo, and C. Yuan, *A Characteristic Set Method for Ordinary Difference Polynomial Systems*, Journal of Symbolic Computation 44 (3), 242-260 (2009).

Maple packages for the analysis of linear systems of partial difference equations and applications

D. Robertz[1]

[1] *Centre for Mathematical Sciences, Plymouth University, 2-5 Kirkby Place, Drake Circus, Plymouth PL4 8AA, UK, daniel.robertz@plymouth.ac.uk*

This talk reviews work by the speaker and coauthors on Maple packages for the analysis of linear systems of partial difference equations and related applications [6, 11, 7, 8, 2].

The Maple package `LDA` [6, 8] has been developed by V. P. Gerdt and the speaker since 2005. It implements algorithms for computing involutive bases [4] for linear difference ideals and, more generally, for submodules of finitely generated free left modules over (not necessarily commutative) rings of difference operators with coefficients in a difference field of characteristic zero.

A first application is the symbolic generation of finite difference schemes for linear PDEs [6, 8]. An elementary integration method is applied to the integral of the corresponding conservation equation, and in the resulting difference equations the partial derivatives of the unknown function are eliminated in favor of the unknown function itself. Following this idea, standard difference schemes for the Laplace, heat, wave, and advection equations and several difference schemes for the Burgers' and Falkowich-Kármán equations have already been generated symbolically in [5]. A second application is the reduction of Feynman integrals, which satisfy certain linear recurrence relations. Another application is a formal computational check of consistency of finite difference approximations of linear systems of PDEs [7].

The Maple package `OreModules` [2] has been developed by F. Chyzak, A. Quadrat and the speaker since 2003. It implements methods of module theory and homological algebra for Ore algebras. Modules over rings of difference operators form a special case to which these methods can be applied. The available procedures allow checks for various structural properties of systems of linear difference equations using an algebraic analysis approach, cf., e.g., [1, 10, 12, 13], for instance, controllability and parametrizability of the behavior.

Both Maple packages `LDA` and `OreModules` are freely available [6], [2].

References

[1] F. Chyzak, A. Quadrat and D. Robertz, *Effective algorithms for parametrizing linear control systems over Ore algebras*, Appl. Algebra Engrg. Comm. Comput. **16**, 5, pp. 319–376 (2005).

[2] F. Chyzak, A. Quadrat and D. Robertz, `OreModules`*: a symbolic package for the study of multidimensional linear systems*, in: J. Chiasson and J.-J. Loiseau (eds.), *Applications of time delay systems*, vol. 352 of Lecture Notes in Control and Inform. Sci., pp. 233–264, Springer, Berlin, 2007. Cf. also `http://wwwb.math.rwth-aachen.de/OreModules`.

[3] R. M. Cohn, *Difference algebra*, John Wiley & Sons, New York-London-Sydney, 1965.

[4] V. P. Gerdt, *Involutive Algorithms for Computing Gröbner Bases*, in: S. Cojocaru, G. Pfister and V. Ufnarovski (eds.), *Computational Commutative and Non-Commutative Algebraic Geometry*, NATO Science Series, pp. 199–225, IOS Press, 2005.

[5] V. P. Gerdt, Y. A. Blinkov and V. V. Mozzhilkin, *Gröbner Bases and Generation of Difference Schemes for Partial Differential Equations*, Symmetry, Integrability and Geometry: Methods and Applications **2**, 26 (2006).

[6] V. P. Gerdt and D. Robertz, *A Maple Package for Computing Gröbner Bases for Linear Recurrence Relations*, Nucl. Instr. Meth. Phys. Res. A **559**, 1, pp. 215–219 (2006). For the Maple package `LDA` cf. also `http://wwwb.math.rwth-aachen.de/Janet`.

[7] V. P. Gerdt and D. Robertz, *Consistency of Finite Difference Approximations for Linear PDE Systems and its Algorithmic Verification*, in: S. M. Watt (ed.), *Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation, TU München, Germany*, pp. 53–59, 2010.

[8] V. P. Gerdt and D. Robertz, *Computation of Difference Gröbner Bases*, Comput. Sci. J. Moldova **20**, 2 (59), pp. 203–226 (2012).

[9] A. Levin, *Difference algebra*, vol. 8 of Algebra and Applications, New York, Springer, 2008.

[10] U. Oberst, *Multidimensional constant linear systems*, Acta Appl. Math. **20**, 1-2, pp. 1–175 (1990).

[11] D. Robertz, *Janet bases and applications*, in: M. Rosenkranz and D. Wang (eds.), *Gröbner bases in symbolic analysis*, vol. 2 of Radon Ser. Comput. Appl. Math., pp. 139–168, Walter de Gruyter, Berlin, 2007. Cf. also `http://wwwb.math.rwth-aachen.de/Janet`.

[12] D. Robertz, *Recent progress in an algebraic analysis approach to linear systems*, Multidimens. Systems Signal Process. **26**, 2, pp. 349–388 (2015).

[13] E. Zerz, *Topics in multidimensional linear systems theory*, vol. 256 of Lecture Notes in Control and Information Sciences, Springer, London, 2000.

On Computing Rational Generating Function of a Solution to the Cauchy Problem of Difference Equation

A.A. Kytmanov[1], A.P. Lyapin[2]

[1] *Siberian Federal University, Russia, aakytm@gmail.com*
[2] *Siberian Federal University, Russia, LyapinAP@yandex.ru*

Algorithms for computing rational generating functions of solutions of one-dimensional difference equations are well-known and easy to implement. We propose an algorithm for computing rational generating functions of solutions of two-dimensional difference equations in terms of initial data of the corresponding initial value problems. The crucial part of the algorithm is the reconstruction of infinite one-dimensional initial data on the basis of finite input data. The proposed technique can be used for the development of similar algorithms in higher dimensions. We furnish examples of implementation of the proposed algorithm.

The one-dimensional case is well-studied (see [1, 2]) due to the absence of geometric obstacles. In [3], A. Moivre considered the power series

$$f(0)+f(1)z+\ldots+f(k)z^k+\ldots$$

with the coefficients $f(0), f(1), \ldots$ satisfying the difference equation

$$c_m f(x+m)+c_{m-1}f(x+m-1)+\ldots+c_0 f(x)=0, \quad x=0,1,2\ldots, \qquad (1)$$

where $c_m \neq 0$, and $c_j \in \mathbb{C}$ are constants. He proved that this series always represents a rational function (De Moivre's Theorem, [3]).

In the multidimensional case, which is not adequately explored (see [4, 5, 6, 7]), the rational generating functions are the most useful class of generating functions according to the Stanley's hierarchy (see [8]). A broad class of two-dimensional sequences that lead to rational generating functions is well-known in the enumerative combinatorics. For example, one can consider the problem of finding a number of lattice paths, the problem on generating trees with marked labels, Bloom's strings, a number of placement of the pieces on the chessboard etc. (see [9, 10, 11]).

Generating functions for multiple sequences with elements which could be expressed in terms of rational, exponential functions or gamma function, form a wide class of hypergeometric-type functions [12, 13]. Their study leads to the problem of solving overdetermined systems of linear equations with polynomial coefficients.

A multidimensional analogue of the De Moivre Theorem was formulated and proved in [15]. We now give some definitions and notations that we will need for formulating the main result.

Let $x = (x_1, \ldots, x_n) \in \mathbb{Z}^n$, where $\mathbb{Z}^n = \mathbb{Z} \times \ldots \times \mathbb{Z}$ is the n-dimensional integer lattice. Let $A = \{\alpha\}$ be a finite set of points in $\mathbb{Z}^n$. Let $f(x)$ be a function of integer arguments $x = (x_1, \ldots, x_n)$ with constant coefficients c_α. By a difference equation with respect to the unknown function $f(x)$ we call the equation of the form

$$\sum_{\alpha \in A} c_\alpha f(x+\alpha) = 0. \tag{2}$$

In the present work we consider the case when the set A belongs to the positive octant $\mathbb{Z}_0^n = \{(x_1, \ldots, x_n), x_i \in \mathbb{Z}, x_i \geq 0, i = 1, \ldots, n\}$ of the integer lattice and satisfies to the condition:

There exists a point $m = (m_1, \ldots, m_n) \in A$ such that for any $\alpha \in A$ the inequalities

$$\alpha_j \leq m_j, \ j = 1, 2, \ldots, n \tag{3}$$

hold.

Denote the *characteristic polynomial* of (2) by

$$P(z) = \sum_{\alpha \in A} c_\alpha z^\alpha = \sum_{\alpha \in A} c_{\alpha_1, \ldots, \alpha_n} z_1^{\alpha_1} \cdots z_n^{\alpha_n}.$$

The generating function (or the z-transformation) of the function $f(x)$ in integer variables $x \in \mathbf{Z}_0^n$ is defined as follows:

$$F(z) = \sum_{x \geq 0} \frac{f(x)}{z^{x+I}}, \quad \text{where } I = (1, \ldots, 1).$$

Define the «initial data set» for the difference equation (2) that satisfies the condition (3), as follows:

$$X_0 = \{\tau \in \mathbb{Z}^n, \tau \geq 0, \ \tau \not\geq m\}.$$

Here $\not\geq$ means that the point τ belongs to the complement of the set defined by the system of inequalities

$$\tau_j \geq m_j, \ j = 1, \ldots, n.$$

The initial value problem is set up as follows: we need to find the solution $f(x)$ of the difference equation (2), which coincides with a given function $\varphi(x)$ on X_0:

$$f(x) = \varphi(x), \ x \in X_0. \tag{4}$$

It is easy to show (see, e.g., [6]), that if the condition (3) holds, then the initial value problem (2), (4) has the unique solution. The solvability of the problem (2), (4) without the constraints (3) has been studied in [4].

We now proceed with some more notations that we will need later on.

Let $J=(j_1,\dots,j_n)$, where $j_k\in\{0,1\}$, $k=1,\dots,n$, be an ordered set. With each such set J we associate the face Γ_J of the n-dimensional integer parallelepiped $\Pi_m=\{x\in\mathbb{Z}^n : 0\le x_k\le m_k, k=1,\dots,n\}$ as follows:

$$\Gamma_J=\{x\in\Pi_m, x_k=m_k, \text{ if } j_k=1, \text{and } x_k<m_k, \text{ if } j_k=0\}. \tag{5}$$

For example, $\Gamma_{(1,\dots,1)}=\{m\}$ and $\Gamma_{(0,\dots,0)}=\{x\in\mathbb{Z}^n, 0\le x_k<m_k,\ k=1,\dots,n\}$.

It is easy to check that $\Pi_m=\bigcup\limits_J\Gamma_J$ and for any J,J' the corresponding faces do not intersect: $\Gamma_J\cap\Gamma_{J'}=\emptyset$.

Let $\Phi(z)=\sum\limits_{\tau\ge 0.\tau\not\ge m}\frac{\varphi(\tau)}{z^{\tau+I}}$ be the generating function of the initial data of the solution of (2), (4). With each point $\tau\in\Gamma_J$ we associate the series

$$\Phi_{\tau,J}(z)=\sum_{y\ge 0}\frac{\varphi(\tau+Jy)}{z^{\tau+Jy+I}},$$

and with each face Γ_J we associate the series

$$\Phi_J(z)=\sum_{\tau\in\Gamma_J}\Phi_{\tau,J}(z).$$

If we extend the domain of $\varphi(x)$ by zero on $\mathbb{Z}^n_+\setminus X_0$, then the generating function of the initial data can be written down as the sum

$$\Phi(z)=\sum_J\Phi_J(z)=\sum_J\sum_{\tau\in\Gamma_J}\Phi_{\tau,J}(z).$$

Theorem 1. The generating function $F(z)$ of the solution of the problem (2),(4) under the assumption (3) and the generating function $\Phi(z)$ of the initial data are connected by the formula

$$P(z)F(z)=\sum_J\sum_{\tau\in\Gamma_J}\Phi_{\tau,J}(z)P_\tau(z), \tag{6}$$

where $P_\tau(z)=\sum\limits_{\alpha\le m,\alpha\not\le\tau}c_\alpha z^\alpha$ are polynomials.

For $n=1$ it is easy to verify the statement of the Theorem 1.

For $n=2$ Theorem 1 was proved in [14] in connection with studying the rational Riordan arrays. For $n>1$ the proof was given in [15]. The properties of generating function of solutions of a difference equation in rational cones of integer lattice were studied by T. Nekrasova (see, e.g., [16]).

Theorem 1 yields the following multidimensional analog of the De Moivre Theorem that is essential for the construction of algorithm:

Theorem 2. The generating function $F(z)$ of the solution of the initial value problem (2), (4) under the assumption (3) is rational if and only if the generating function $\Phi(z)$ of the initial data is rational.

The proof of Theorem 2 was given in [15].

For $n = 1$ the expression for the generating function consists of a finite number of terms, which makes the corresponding algorithm and computational procedure trivial. In this case the input data consists of two finite sets of numbers, namely: coefficients of the difference equation and the initial data. The output data of the algorithm is a rational function.

In the case when $n > 1$, the initial data set X_0 is infinite. For $n = 2$ the algorithm for computing the generating function $F(z)$ can be reduced to computation of a finite number of one-dimensional generating functions of sequences with elements along the coordinate axes. These elements are uniquely determined by coefficients of the corresponding one-dimensional difference equation and by finite set of the corresponding initial data (that is different for each sequence).

We use theorem 1 for the development some algorithms for computing rational generation functions in the lattice paths problem, the level generation trees problem in the dimension higher than two.

Example. Bloom studies the number of singles in all 2^x x-length bit strings [11], where a single is any isolated 1 or 0, i.e. any run of length 1. Let $r(x,y)$ be the number of x-length bit strings beginning with 0 and having y singles. Apparently $r(x,y) = 0$ if $x < y$.

In [11] D. Bloom proves that $r(x,y)$ is a solution to the Cauchy problem

$$r(x+2,y+1) - r(x+1,y+1) - r(x+1,y) - r(x,y+1) + r(x,y) = 0$$

with the initial data $\varphi(0,0) = 1, \varphi(1,0) = 0, \varphi(x,0) = \varphi(x-1,0) + \varphi(x-2,0),\ x \geq 2, \varphi(0,y) = 0,\ y \geq 1, \varphi(1,1) = 1, \varphi(1,y) = 0,\ y \geq 2.$

The result is the generating function of the considered initial value problem:

$$F(z,w) = \frac{z-1}{z^2w - zw - w - z + 1}.$$

Acknowledgements. The research was partially supported by the state order of the Ministry of Education and Science of the Russian Federation for Siberian Federal University (task 1.1462.2014/K, first author) and by the Russian Foundation for Basic Research, projects 15-31-20008-mol_a_ved, 15-01-00277-a (the first author) and 14-01-00283-a (first and second authors).

References

[1] A.O. Gelfond, *The calculus of finite differences*, Moscow, KomKniga (2006).

[2] R.F. Isaacs, *A finite difference function theory*, Univ. Nac. Tucuman. **2**, pp. 177–201 (1941).

[3] A. de Moivre, *De Fractionibus Algebraicis Radicalitate Immunibus ad Fractiones Simpliciores Reducendis, Deque Summandis Terminis Quarumdam Serierum Aequali Intervallo a Se Distantibus*, Philosophical Transactions, **32**, pp. 162–178 (1722).

[4] M. Bousquet-Mélou and M. Petkovšek, *Linear recurrences with constant coefficients: the multivariate case*, Discrete Mathematics. **225**, pp. 51–75 (2000).

[5] E.K. Leinartas, *Multiple Laurent series and difference equations*, Siberian Math. J. **45** (2), pp. 321–326 (2004).

[6] E.K. Leinartas, *Multiple Laurent series and fundamental solutions of linear difference equations*, Siberian Math. J. **48** (2), pp. 268–272 (2007).

[7] E.K. Leinartas, M. Passare and A.K. Tsikh, *Multidimensional versions of Poincare's theorem for difference equations*, Sbornik: Mathematics **199** (10), pp. 1505–1521 (2008).

[8] R. Stanley, *Enumerative combinatorics*, Cambridge University Press, Cambridge (1996).

[9] G.P. Egorychev, *Integral representation and the computation of combinatorial sums*, Nauka, Novosibirsk (1977) (in Russian).

[10] D. Baccherini, D. Merlini and R. Sprugnoli, *Level generation trees and proper Riordan arrays*, Applicable Analysis and Discrete Mathematics **2**, pp. 69–91 (2008).

[11] D.M. Bloom, *Singles in a sequence of coin tosses*, Coll. Math. J. **29** (2), pp. 120–127 (1998).

[12] T.M. Sadykov, *On a multidimensional system of differential hypergeometric equations*, Siberian Math. J. **39** (5), pp. 986–997 (1998).

[13] A. Dickenstein, T.M. Sadykov, *Algebraicity of solutions to the Mellin system and its monodromy*, Doklady Mathematics **75** (1), pp. 80–82 (2007).

[14] A.P. Lyapin, *Riordan's arrays and two-dimensional difference equations*, Journal of Siberian Federal University. Mathematics & Physics, **2(2)**, pp. 210–220 (2009).

[15] E.K. Leinartas, A.P. Lyapin, *On the Rationality of Multidimentional Recusive Series*, Journal of Siberian Federal University. Mathematics & Physics, **2(4)**, pp. 449–455 (2009).

[16] T.I. Nekrasova, *On the Cauchy Problem for Multidimensional Difference Equations in Rational Cone*, Journal of Siberian Federal University. Mathematics & Physics **8(2)**, pp. 184–191 (2015).

Computing difference algebraic relations among solutions of linear differential equations

M. Wibmer[1]

[1] *University of Pennsylvania, Philadelphia, USA, wibmer@math.upenn.edu*

While the classical Picard-Vessiot theory is concerned with the algebraic relations among the solutions of linear differential or difference equations, the parameterized Picard-Vessiot theory deals with algebraic relations among the solutions and their transformations under various operations like differentiation, shifting or scaling.

For example, the solution $J_\alpha(x)$ of Bessel's differential equation

$$x^2y'' + xy' + (x^2 - \alpha^2)y = 0$$

satisfies the difference algebraic relation

$$xJ_{\alpha+2}(x) - 2(\alpha+1)J_{\alpha+1}(x) + xJ_\alpha(x) = 0.$$

This relation is witnessed by the associated Galois group, which is a difference algebraic groups, i.e., a group defined by difference equations. We will provide a computational perspective on how to compute these groups and find the corresponding difference algebraic relations.

References

[1] L. Di Vizio, Ch. Hardouin and M. Wibmer, *Difference Galois theory of linear differential equations*, Adv. Math. **260**, pp. 1-58 (2014)

[2] L. Di Vizio, Ch. Hardouin and M. Wibmer, *Difference algebraic relations among solutions of linear differential equations*, to appear in JIMJ

S6
Computer Algebra for Dynamical Systems and Celestial Mechanics

A Case Study on the Parametric Occurrence of Multiple Steady States

H. Errami[1], V. Gerdt[2], D. Grigoriev[3], M. Košta[4], O. Radulescu[5], T. Sturm[6,4], A. Weber[1]

[1] *Universität Bonn, Bonn, Germany; {errami,weber}@cs.uni-bonn.de*
[2] *Joint Institute for Nuclear Research, Dubna, Russia*
[3] *CNRS, Mathématiques, Université de Lille, Villeneuve d'Ascq, France*
[4] *Max-Planck-Institut für Informatik, Saarbrücken, Germany*
[5] *DIMNP UMR CNRS/UM 5235, University of Montpellier, Montpellier, France;*
[6] *CNRS, LORIA, Inria, and University of Lorraine, Nancy, France*

Bistability— or more generally multistationarity—has important consequences on the capacity of signaling pathways to process biological signals. Bistable switches can act as memory circuits storing the information needed for later stages of processing [19]. The response of bistable signaling pathways show hysteresis, namely dynamic and static lags between input and output. Because of hysteresis, one can have in the same time sharp, all or nothing response and protection against chatter noise. Bistability of signaling usually occurs as a result of activation of upstream signaling proteins by downstream components [2]. A different mechanism for producing bistability in signaling pathways was proposed by Kholodenko [14]. In this mechanism the cause of bistability are multiple phosphorylation/dephosphorylation cycles that share enzymes. A simple, two steps phosphorylation/dephosphorylation cycle is capable of ultrasensitivity, a form of all or nothing response with no hysteresis (Goldbeter-Koshland mechanism). In multiple phosphorylation/dephosphorylation cycles, enzyme sharing provides competitive interactions and positive feedback that ultimately leads to bistability.

Algorithmically the task is to find the positive real solutions of a parameterized system of polynomial or rational systems, since the dynamics of the network is given by polynomial systems—arising from mass action kinetics—or rational functions—arising in signaling networks when some some intermediates of the reaction mechanisms are reduced. Due to the high computational complexity of this task [10] considerable work has been done to use specific properties of networks and to investigate the potential of bistability (or more general, multistationarity) of a biological network out of the network structure and only to determine whether there exist certain rate constants such that there are multiple steady states instead of coming up with a semi-algebraic description of the range of parameters yielding this property. These approaches can be traced back to the origins of Feinberg's *chemical reaction network theory* (CRNT) whose main result is that networks of deficiency 0 have a unique positive steady state for all rate constants [9, 5]. For

clever ways to use CRNT and other graph theoretic methods to determine in contrast the potential of multiple positive steady states we refer to [4, 16, 11] and to [12] for a survey.

However, given a bistable mechanism it is important to compute the bistability domains in *parameter space*, namely the parameter values for which there are more than one stable steady states. The size of bistability domains gives the spread of the hysteresis and quantifies the robustness of the switches. For this purpose the work of Wang and Xia [15] is relevant: they used symbolic computation tools to determine the number of steady states and their stability of several systems—and they reported results up to a 5-dimensional system using specified parameter values—but their method is extensible to parametric questions. However, we are not aware of work on higher-dimensional systems for this context.

In this paper we use an 11-dimensional model of a mitogen-activated protein kinases (MAPK) cascade [14] as a case study to investigate properties of the system and algorithmic methods towards the goal of semi-algebraic descriptions of parameter regions for which multiple positive steady states exist.

The MapK Network and the Arising System of Polynomials. The model of the MAPK cascade we are investigating can be found in the Biomodels database [13] as number 26 and is given by the following set of differential equations. We have renamed the species names into $x_1,\ldots,x_{11}$ and the rate constants into $k_1,\ldots,k_{16}$ to facilitate reading:

$$\begin{aligned}
\dot{x_1} &= k_2x_6 + k_{15}x_{11} - k_1x_1x_4 - k_{16}x_1x_5\\
\dot{x_2} &= k_3x_6 + k_5x_7 + k_{10}x_9 + k_{13}x_{10} - x_2x_5(k_{11}+k_{12}) - k_4x_2x_4\\
\dot{x_3} &= k_6x_7 + k_8x_8 - k_7x_3x_5\\
\dot{x_4} &= x_6(k_2+k_3) + x_7(k_5+k_6) - k_1x_1x_4 - k_4x_2x_4\\
\dot{x_5} &= k_8x_8 + k_{10}x_9 + k_{13}x_{10} + k_{15}x_{11} - x_2x_5(k_{11}+k_{12}) - k_7x_3x_5 - k_{16}x_1x_5\\
\dot{x_6} &= k_1x_1x_4 - x_6(k_2+k_3)\\
\dot{x_7} &= k_4x_2x_4 - x_7(k_5+k_6)\\
\dot{x_8} &= k_7x_3x_5 - x_8(k_8+k_9)\\
\dot{x_9} &= k_9x_8 - k_{10}x_9 + k_{11}x_2x_5\\
\dot{x_{10}} &= k_{12}x_2x_5 - x_{10}(k_{13}+k_{14})\\
\dot{x_{11}} &= k_{14}x_{10} - k_{15}x_{11} + k_{16}x_1x_5
\end{aligned}$$

Using the left-null space of the stoichiometric matrix under positive conditions as conservation constraint [8] we obtain the following three linear conservation

constraints:

$$\begin{aligned} x_5 - k_{17} + x_8 + x_9 + x_{10} + x_{11} &= 0, \\ x_4 - k_{18} + x_6 + x_7 &= 0, \\ x_1 - k_{19} + x_2 + x_3 + x_6 + x_7 + x_8 + x_9 + x_{10} + x_{11} &= 0, \end{aligned}$$

where k_{17}, k_{18}, k_{19} are new constants computed from the initial data.

Computing complex solutions using homotopy solvers We estimate all parameters except k_{19} with values from Biomodels database as follows:

$$\begin{array}{lllll} k_1 = 0.02, & k_4 = 0.032, & k_7 = 0.045, & k_9 = 0.092, & k_{15} = 0.086, \\ k_2 = 1, & k_3 = 0.01, & k_5 = 1, & k_6 = 15, & k_8 = 1, \\ k_{10} = 1, & k_{11} = 0.01, & k_{12} = 0.01, & k_{14} = 0.5, & k_{13} = 1, \\ k_{16} = 0.0011, & k_{17} = 100, & k_{18} = 50. & & \end{array}$$

Using the homotopy solver Bertini [1] we obtained the following results using for k_{19} different parameter values found in the literature: For the parameter values as above and $k_{19} = 500$ we obtained 6 solutions, of which 3 were positive real solutions. For $k_{19} = 200$, a single positive solutions was obtained.

Determination of Parametric Multiple Steady States. Our focus to analyze the system for multiple positive steady states is on methods based on real quantifier elimination, which directly can deal with the quest of multiple positive real solutions even in the presence of parameters. Although the method can handle arbitrary numbers of parameters in principle, only one parameter has been left free to come up with feasible computations.

Using a combination of Redlog [7, 17, 18, 6] and Qepcad B [3] we have obtained the following results (using the estimates for the parameters except of k_{19} as above):

1. For all positive choices of k_{19}—extending to infinity—there is at least one positive solution for $(x_1, \ldots, x_{11})$.
2. There is a breaking point β around $k_{19} = 409.253$ where the system changes its qualitative behavior. We have exactly computed β as a real algebraic number. For $k_{19} < \beta$ there is exactly one positive solution for $(x_1, \ldots, x_{11})$. For $k_{19} > \beta$ there are at least 3 and at most 3^{11} positive solutions for $(x_1, \ldots, x_{11})$.

The overall computation time for this parametric analysis has been les than 5 minutes.

Determining the Stability of the Fixed Points. For the numeric approximations of the fixed points we numerically computed the eigenvalues of the Jacobian using Maple. For $k_{19} = 200$ the single positive fixed point could be shown to be stable in this way, whereas for $k_{19} = 500$ one of the three positive fixed points could be shown to be unstable whereas two could be shown to be stable. Hence for $k_{19} = 500$ the system is indeed bistable.

A verification of the stability of the fixed points using the exact real algebraic numbers and the Routh-Hurwitz criterion seems to be out of range of current methods for this example.

Conclusion and Future Work. Although the goal of semi-algebraic description of the range of some parameters yielding bistable behavior could not be achieved for the 11-dimensional system, which was used for the case study, our case study shows that one is not too far off.

As there are many very relevant systems having dimensions between 10 and 20 it seems to be worth the effort to enhance the algorithmic methods and to come up with improved implementations of them to solve this very important applications problem for symbolic computation. In addition to improving the real quantifier elimination methods, which can deal with the question of positive real solutions in a parametric way directly, using methods that deal with complex solutions first (such as Gröbner bases or regular chain methods) are a topic of future research. A challenge for the latter methods are the parametric determination of the positive real solutions out of the descriptions of the complex solutions.

Acknowledgements. D. Grigoriev is grateful to the grant RSF 16-11-10075 and to MCCME for wonderful working conditions and inspiring atmosphere. M. Košta has been supported by the DFG/ANR Project STU 483/2-1 SMArT. For our QE-related computations we used two great free software tools: GNU Parallel for distributing computations on several processors, and yEd for visualization of CAD trees. H. Errami, A. Weber, and O. Radulescu thank the French-German Procope-DAAD program for partial support of this research.

References

[1] D. J. Bates, J. D. Hauenstein, A. J. Sommese, and C. W. Wampler. Bertini: Software for numerical algebraic geometry. Available at bertini.nd.edu with permanent doi:

dx.doi.org/10.7274/R0H41PB5.

[2] U. S. Bhalla and R. Iyengar. Emergent properties of networks of biological signaling pathways. *Science*, 283(5400):381–387, 1999.

[3] C. W. Brown. QEPCAD B: a program for computing with semi-algebraic sets using CADs. *ACM SIGSAM Bulletin*, 37(4):97–108, 2003.

[4] C. Conradi, D. Flockerzi, and J. Raisch. Multistationarity in the activation of a MAPK: parametrizing the relevant region in parameter space. *Math. Biosci.*, 211(1):105–31, jan 2008.

[5] G. Craciun, A. Dickenstein, A. Shiu, and B. Sturmfels. Toric dynamical systems. *Journal of Symbolic Computation*, 44(11):1551–1565, 2009.

[6] A. Dolzmann, A. Seidl, and T. Sturm. Efficient projection orders for CAD. In J. Gutierrez, editor, *Proceedings of the 2004 International Symposium on Symbolic and Algebraic Computation (ISSAC 2004)*, pages 111–118. ACM Press, New York, NY, July 2004.

[7] A. Dolzmann and T. Sturm. Redlog: Computer algebra meets computer logic. *ACM SIGSAM Bulletin*, 31(2):2–9, June 1997.

[8] I. Famili and B. Ø. Palsson. The convex basis of the left null space of the stoichiometric matrix leads to the definition of metabolically meaningful pools. *Biophys. J.*, 85(1):16–26, 2003.

[9] M. Feinberg. Stability of complex isothermal reactors–I. the deficiency zero and deficiency one theorems. *Chemical Engineering Science*, 42(10):2229–2268, 1987.

[10] D. Grigoriev and N. N. Vorobjov. Solving systems of polynomial inequalities in subexponential time. *Journal of Symbolic Computation*, 5(1-2):37–64, Feb. 1988.

[11] M. Johnston. A note on" MAPK networks and their capacity for multistationarity due to toric steady states". *arXiv Prepr. arXiv1407.5651*, pages 1–13, 2014.

[12] B. Joshi and A. Shiu. A Survey of Methods for Deciding Whether a Reaction Network is Multistationary. *Math. Model. Nat. Phenom.*, 10(5):47–67, aug 2015.

[13] C. Li, M. Donizelli, N. Rodriguez, H. Dharuri, L. Endler, V. Chelliah, L. Li, E. He, A. Henry, M. I. Stefan, J. L. Snoep, M. Hucka, N. Le Novère, and C. Laibe. BioModels database: An enhanced, curated and annotated resource for published quantitative kinetic models. *BMC Systems Biology*, 4:92, Jan. 2010.

[14] N. I. Markevich, J. B. Hoek, and B. N. Kholodenko. Signaling switches and bistability arising from multisite phosphorylation in protein kinase cascades. *J. Cell Biol.*, 164(3):353–359, 2004.

[15] F. Paris, D. Wang, and B. Xia. Stability analysis of biological systems with real solution classification. In *ISSAC '05 Proc. 2005 Int. Symp. Symb. Algebr. Comput.*, pages 354–361, Beijing, China, 2005. ACM.

[16] M. Pérez Millán and A. G. Turjanski. MAPK's networks and their capacity for multistationarity due to toric steady states. *Math. Biosci.*, 262:125–37, 2015.

[17] A. Seidl. *Cylindrical Decomposition Under Application-Oriented Paradigms*. PhD thesis, Universität Passau, 94030 Passau, Germany, Mar. 2006.

[18] A. Seidl and T. Sturm. A generic projection operator for partial cylindrical algebraic decomposition. In R. Sendra, editor, *Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation (ISSAC 03), Philadelphia, Pennsylvania*, pages 240–247. ACM Press, New York, NY, 2003.

[19] G. Weng, U. S. Bhalla, and R. Iyengar. Complexity in biological signaling systems. *Science*, 284(5411):92–6, 1999.

Quantitative analysis of competition models

C. Chiralt[1], A. Ferragut[1], A. Gasull[2], P. Vindel[1]

[1] *Universitat Jaume I, Spain, chiralt@mat.uji.es, ferragut@uji.es, vindel@uji.es*
[2] *Universitat Autònoma de Barcelona, Spain, gasull@mat.uab.cat*

We study the planar Lotka-Volterra differential system of competition between two competing species having a saddle in the first quadrant. We show that, under certain conditions on the parameters of the system, one of the separatrices of the saddle divides the first quadrant in two, and hence depending on the initial conditions one of the species will extinct because the ω-limits are attracting nodes on the axes. We study the probability of the species of surviving depending on the initial choice of the parameters, providing an index κ.

Greedy trajectories of Plancherel processes on two dimensional Young and Schur graphs

N. Vasilyev[1], V. Duzhin[2]

[1] *St.Petersburg department of Steklov Institute of mathematics RAS, Russia, vasiliev@pdmi.ras.ru*
[2] *St.Petersburg Electrotechnical University, Russia, vduzhin.science@gmail.com*

The sequences of the greedy branching or greedy trajectories are a special kind of infinite paths of Bratteli-Vershik diagrams provided by a certain Markov process. In these trajectories, the edge connecting two adjacent levels corresponds to the maximum transition probability of Markov process. There is an important special case of such process named the Plancherel process on 2D Young graph. The greedy trajectories of this dynamical system allows to investigate the asymptotics of the maximum dimensions of irreducible representations of symmetric group. The similar trajectories on the Schur graph allows to obtain the similar results for maximum dimensions of projective representations of symmetric group.

We present the results of a computer investigation of asymptotics for maximum dimensions of linear and projective representations of the symmetric group. This problem reduces to the investigation of standard and strict Young diagrams of maximum dimensions. We constructed some sequences for both standard and strict Young diagrams with extremely large dimensions [2]. These sequences provide the estimations of maximum normalized dimension of Young diagrams. These estimations are agreed with the Vershik conjecture [1] about the existence of the limit of maximum normalized dimensions of 2D Young diagrams. Note that this conjecture has not been proved yet. We studied the growth and oscillations of the normalized dimension function in sequences of Young diagrams. Our approach is based on analyzing the finite differences of their normalized dimensions [3]. This analysis also allows us to give much more precise estimation of the hypothetical limit constants.

There are no known exact analogue of the plancherel process for the case of 3D Young diagrams. However, there is a special process on 3D Young graph which supposedly has the property of asymptotical centrality instead of exact centrality. We present the results of computer investigation of greedy trajectories corresponding to this process. Some geometric properties of Young diagrams along these trajectories will be presented as well. Also we present a special package for manipulations with 2D and 3D Young diagrams and Young tableaux which was developed in the frame of this work.

This work was supported by grant RSF 14-11-00581.

References

[1] A. M. Vershik and S. V. Kerov. "Asymptotic behavior of the maximum and generic dimensions of irreducible representations of the symmetric group." Funktsional. Anal. i Prilozhen., 19(1):25-36, 1985.

[2] Vasilyev N. N., Duzhin V. S. Building Irreducible Representations of a Symmetric Group S(n) with Large and Maximum Dimensions. Informatsionno-upravliaiushchie sistemy [Information and Control Systems], 2015, no. 3, pp. 17-22 (In Russian). doi:10.15217/issn1684-8853.2015.1.17

[3] Vasiliev N. N., Duzhin V. S. A Study of the Growth of the Maximum and Typical Normalized Dimensions of Strict Young Diagrams, 216 Journal of Mathematical Sciences 53-64 (2016). http://doi.org/10.1007/s10958-016-2887-x

Symbolic Dynamics, Mixing and Entropy in the Three-Body Problem

A. Mylläri [1], V. Orlov[2] , A. Chernin [3], T. Mylläri[1]

[1] *St. George's University, Grenada, West Indies, amyllari@sgu.edu*
[2] *Sobolev Astronomical Institute, St. Petersburg State University, Russia*
[3] *Sternberg Astronomical Institute, Moscow State University, Russia,*

We use symbolic dynamics in the equal mass free-fall three-body problem. Different methods to construct (in the process of numerical integration of trajectories) symbolic sequences allow one to demonstrate (and illustrate on the Agekian-Anosova map) mixing, estimate entropies (Shannon, Markov and others), plot binary collision curves, etc.

We use Agekian-Anosova map (see Fig. 1) for the partitioning. It was used to specify initial conditions so that to consider all possible configugurations: two bodies are placed in the points (-0.5; 0) and (0.5; 0), then to consider all possible geometric configurations, the third body should be placed inside the region D (Fig. 1). The system is projected to the region D according to the relative distances between bodies. There are six different projections possible, thus we get sequences constructed from the alphabet {1; 2; 3; 4; 5; 6}. We also used partitions of the homology region D into 3 and 4 parts, having alphabet of 3 and 4 symbols correspondingly. A second approach is to fix some dynamical states (binary encounters, triple encounters etc.) during the evolution of the triple system. We used double and triple encounters to construct two more sequences with alphabets {1; 2; 3}.

Figure 2 shows typical distribution of entropy. To illustrate sensitivity to initial conditions, one can plot a sequence of images visualizing consequently first, second, third, etc. symbol in the sequence. Example (corresponding to 24^{th} symbol in the sequence) is given on the Figure 3.

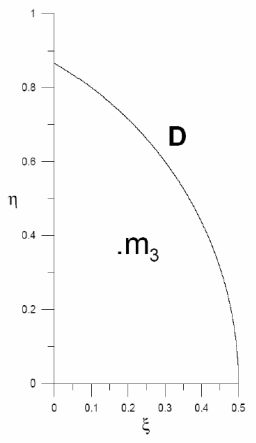


Figure 1: The Agekian-Anosova map (homology region D).

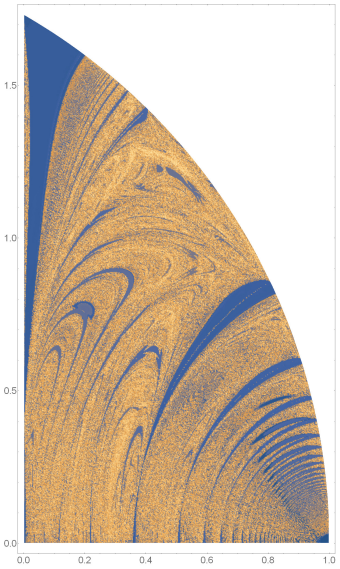


Figure 2: Values of the (Shannon) entropy in different parts of the Agekian-Anosova map are represented by different colors. Low values are shown in blue; high values are shown in light brown.

Figure 3: Sensitivity to initial conditions: different colors correspond to different symbol #24 in the symbolic sequence.

Global dynamics of Planar Quintic Quasi–homogeneous Polynomial Differential Systems

Y. Tang[1], X. Zhang[2]

[1] *Center for Applied Mathematics and Theoretical Physics, University of Maribor, Krekova 2, Maribor 2000, Slovenia, mathtyl@sjtu.edu.cn,*
[2] *Shanghai Jiao Tong University, Shanghai, China, xzhang@sjtu.edu.cn*

In the qualitative theory of planar polynomial differential systems, there are lots of results on their topological structures. But there are only few class of planar polynomial differential systems whose globally topological phase portraits were completely characterized. We consider quasi–homogeneous polynomial differential systems for their global dynamics. Homogeneous systems are a class of special quasi–homogeneous systems. Many papers have characterized phase portraits of homogeneous polynomial vector fields. Recently, García *et al* [2] provided an algorithm to compute quasi–homogeneous but non–homogeneous polynomial differential systems with a given degree and obtained all the quadratic and cubic quasi–homogeneous but non–homogeneous vector fields. Aziz *et al* [1] characterized all cubic quasi–homogeneous polynomial differential equations which have a center. Liang *et al* [3] classified all quartic quasi–homogeneous but non–homogeneous differential systems, and obtained all their topological phase portraits. Until now the topological phase portraits of all quintic quasi–homogeneous but non–homogeneous differential systems have not been settled. We [4] first characterize all quasi–homogeneous but non–homogeneous planar polynomial differential systems of degree five, and then among which we classify all the ones having a center at the origin. Finally we characterize the global topological phase portraits of quintic quasi–homogeneous but non–homogeneous differential systems.

References

[1] W. Aziz, J. Llibre and C. Pantazi, *Centers of quasi–homogeneous polynomial differential equations of degree three*, Adv. Math. **254**, pp. 233-250 (2014).

[2] B. García, J. Llibre and J. S. Pérez del Río, *Planar quasihomogeneous polynomial differential systems and their integrability*, J. Diff. Eqns. **255**, pp. 3185-3204 (2013).

[3] H. Liang, J. Huang and Y. Zhao, *Classification of global phase portraits of planar quartic quasi–homogeneous polynomial differential systems*, Nonlinear Dynam. **78**, pp. 1659–1681 (2014).

[4] Y. Tang, L. Wang and X. Zhang, *Center of planar quintic quasi– homogeneous polynomial differential systems*, Discrete Contin. Dyn. Syst. **35**, pp. 2177-2191 (2015).

P4 and desingularization of vector fields in the plane

J.C. Artes[1], P. De Maesschalck[2], F. Dumortier[3], C. Herssens, J. Llibre[4]

[1] *Universitat Autonoma de Barcelona, Spain, artes@mat.uab.cat*
[2] *Hasselt University, Belgium, peter.demaesschalck@uhasselt.be*
[3] *Hasselt University, Belgium, freddy.dumortier@uhasselt.be*
[4] *Universitat Autonoma de Barcelona, Spain, llibre@mat.uab.cat*

Similar to the way degenerate singular points of planar curves are desingularized, so can singularities of vector fields in the plane

$$X = f(x,y)\frac{\partial}{\partial x} + g(x,y)\frac{\partial}{\partial y}$$

be desingularized. The idea is to apply a singular change of coordinates so that in the new set of coordinates, the singular point becomes more elementary and the dynamics around the singular points becomes better understandable. This idea is universal and need not be restricted to the plane, however in the plane there is a result on the finiteness of the desingularization process for analytic vector fields. This means that after a number of steps that could be carried out by a computer, the singular points is replaced by an invariant locus containing at most a finite number of semi-elementary singular points. This shows that the local study of singular points can be automated. Singular points can be found numerically in the case of polynomial X, and in that case, the study can be completed with a study at infinity by means of a so-called Poincaré compactification or Poincaré-Lyapunov compactification. We illustrate the implementation with P4 and briefly discuss P5.

References

[1] F. Dumortier, J. Llibre, J.C. Artès, *Qualitative theory of planar differential systems*, Springer-Verlag, Berlin, 2006, ISBN: 3-540-32893-9.

Local invariant sets of analytic vector fields

N. Kruff

RWTH Aachen University, Germany, Lehrstuhl A für Mathematik

In the theory of autonomous ordinary differential equations invariant sets play an important role. In particular, we are interested in local analytic invariant sets near stationary points. Invariant sets of the differential equation correspond to invariant ideals of the associated derivation in the power series algebra. Poincaré-Dulac normal forms are very useful in studying semi-invariants and invariant ideals. We prove that an invariant ideal with respect to a vector field, given in normal form, is already invariant with respect to the semisimple part of its Jacobian at the stationary point. This generalizes a known result about semi-invariants, that is invariant sets of codimension 1. As an application, we consider polynomial systems and bound the total degree of possible polynomial semi-invariants under some generic conditions.

Invariant varieties for rational control systems

C. Schilli[1], E. Zerz[2], V. Levandovskyy[3]

[1] *RWTH Aachen University, Germany, {christian.schilli}@math.rwth-aachen.de*
[2] *RWTH Aachen University, Germany, {eva.zerz}@math.rwth-aachen.de*
[3] *RWTH Aachen University, Germany, {viktor.levandovskyy}@math.rwth-aachen.de*

In [3], polynomially nonlinear state-space systems

$$\dot{x}(t) = f(x(t)) + g(x(t)) \cdot u(t), \quad y(t) = h(x(t)) \tag{1}$$

and given algebraic varieties were considered. A variety V is said to be controlled invariant w.r.t. (1) if we can find a polynomial state feedback law $u(t) = \alpha(x(t))$ that causes the closed loop system $\dot{x}(t) = (f + g\alpha)(x(t))$ to have V as an invariant set. If this task can be achieved by a polynomial output feedback law $u(t) = \beta(y(t))$, then V is called controlled and conditioned invariant. In this talk, we want to generalise this concept from polynomial systems to rational ones and also allow the feedback law to be rational. We give algebraic conditions for a variety to be controlled (and conditioned) invariant for rational control systems and algorithms (using methods from the theory of Gröbner bases), which may decide this and produce corresponding state (or output) feedback laws.

References

[1] C. Schilli, E. Zerz and V. Levandovskyy, *Controlled and conditioned invariant varieties for polynomial control systems with rational feedback*, Submitted to: Proceedings of the 22nd international symposium on mathematical theory of networks and systems, 2016.

[2] C. Schilli, E. Zerz and V. Levandovskyy, *Controlled and conditioned invariant varieties for polynomial control systems*, Proceedings of the 21st international symposium on mathematical theory of networks and systems, pp. 1691-1698, 2014.

[3] E. Zerz and S. Walcher, *Controlled invariant hypersurfaces of polynomial control systems*, Qualitative theory of dynamical systems, vol. 11, pp. 145-158, 2012.

Elementary and Darboux first integrals for planar polynomial vector fields

J. Llibre[1], C. Pantazi[2], S. Walcher[3]

[1] *Universitat Autònoma de Barcelona, Spain, jllibre@mat.uab.cat*
[2] *Universitat Politecnica de Catalunya, Spain, chara.pantazi@upc.edu*
[3] *Lehrstuhl A für Mathematik, RWTH Aachen, Germany, walcher@mathA.rwth.aachen.de*

It is well known (due to Singer's results) that the existence of an elementary first integral (over the field of rational functions) for a planar polynomial vector field implies the existence of a first integral of a special form and also the existence of a particular integrating factor of Darboux type. In this talk we present rather general conditions that guarantee that the existence of an elementary first integral yields to the existence of a Darboux first integral. Moreover, we provide a complete characterization of such vector fields. Additionally, we provide some exceptional cases of vector fields which admit elementary first integral constructed by algebraic functions of degree two or three.

References

[1] J. Chavarriga, H. Giacomini, J. Giné, J. Llibre: *Darboux integrability and the inverse integrating factor.* J. Differential Eqs. **194** (2003), 116–139.

[2] M. Rosenlicht: *Liouville's theorem on functions with elementary integrals.* Pacific J. Math. **24** (1968), 153–161.

[3] M.F. Singer: *Liouvillian first integrals of differential equations.* Trans. Amer. Math. Soc. **333** pp. 673–688 (1992).

Limit cycles in planar polynomial systems

J. Torregrosa

Universitat Autònoma de Barcelona, Spain torre@mat.uab.cat

A particular version of the 16th Hilbert's problem is to estimate the number, $M(n)$, of limit cycles bifurcating from a singularity of center-focus type. The problem to finding lower bounds for $M(n)$ for some concrete n can be done studying the cyclicity for different weak-foci or centers. Since a weak-focus with high order is the most current way to produce high cyclicity, we present systems with few monomials with the highest known weak-focus order. Christopher in [1] proved that under some assumptions the linear parts of the Lyapunov constants with respect to the parameters give the cyclicity of an elementary center. We will show a new approach, namely parallelization, to compute the linear parts of the Lyapunov constants. More concretely, it is showed that parallelization computes these linear parts in a shorter quantity of time than other traditional mechanisms. Christopher's approach can be applied also to the weak-focus case. For even n, the studied polynomial system of degree n was the one obtained by [5] where the highest weak-focus order is n^2+n-2 for $n=4,6,\ldots,18$. Moreover, we provide a system which has a weak-focus with order $(n-1)^2$ for $n\leq 12$. We also show by concrete examples that, in some families, this approach is so powerful and the cyclicity can be obtained in a simple computational way. To show the power of this approach, we study the cyclicity of the holomorphic center $\dot{z}=iz+z^2+z^3+\cdots+z^n$ under general polynomial perturbations of degree n, for $n\leq 13$. We prove that the cyclicity of the holomorphic center is n^2+n-2. This result give the highest lower bound for $M(6),M(7),\ldots,M(13)$ among the existing results.

References

[1] C. Christopher, *Estimating limit cycle bifurcations from centers*, Differential equations with symbolic computation, in: Trends Math., 30, 23–35, 2006.

[2] A. Gasull, J. Giné, and J. Torregrosa. *Center problem for systems with two monomial nonlinearities*, Comm. Pure Appl. Math., 15(2), 577–598, 2016.

[3] H. Liang and J. Torregrosa. *Weak-foci of high order and cyclicity*, Qual. Theory Dyn. Syst., Published on line, 2016.

[4] H. Liang and J. Torregrosa. *Parallelization of the Lyapunov constants and cyclicity for centers of planar polynomial vector fields*, J. Differential Equations, 259, 6494–6509, 2015.

[5] Y. Qiu and J Yang, *On the focus order of planar polynomial differential equations,* J. Differential Equations, 246, 3361–3379, 2009.

A Geometric Approach for Invariant Algebraic Curves in 2D Lotka Volterra Systems I

C.J. Christopher[1], W.M.A. Hussein[2,3]

[1] *School of Computing, Electronics and Mathematics, Plymouth Univeristy, Plymouth, UK, c.christopher@plymouth.ac.uk*
[2] *School of Computing, Electronics and Mathematics, Plymouth University, Plymouth, UK, wuria.hussein@postgrad.plymouth.ac.uk*
[3] *Salahaddin-Hawler University, Kurdistan Region, Iraq, wuria.hussein@su.edu.krd*

In 2001, Moulin-Ollagnier [1, 2] classified all families of two dimensional Lotka-Volterra systems which have invariant algebraic curves. Twenty-five families of such curves were found using an essentially algebraic search. Our interest is to re-evaluate these families in terms of their geometric behavior. Although we are not able to provide a complete geometric proof of Moulin-Ollagnier's result, we are able to give geometric necessary conditions for the possible families of curves of low degree and, in some of these cases, can also prove the sufficiency of these conditions in purely geometric terms. The talk will be in two parts: the first will give the background and some of the tools used and the second will give more detailed examples. We will also show how this geometric understanding can be used to extend the classification of integrable critical points in Lotka Volterra systems started in [3]. This latter application is joint work with Zhaoxia Wang [4].

References

[1] J. Moulin-Ollagnier, *Liouvillian integration of the Lotka-Volterra system*, Qualitative Theory of Dynamical Systems **2**, 2, pp. 307-358 (2001).

[2] J. Moulin-Ollagnier, *Corrections and complements to Liouvillian integration of the Lotka-Volterra system*, Qualitative Theory of Dynamical Systems **5**, 2, pp. 275-284 (2004).

[3] C. Christopher and C. Rousseau, *Normalizable, integrable and linearizable saddle points in the Lotka-Volterra system*, Qualitative Theory of Dynamical Systems **5**, 1, pp. 11-61 (2004).

[4] C. Christopher, W.M.A. Hussein and Z. Wang, *On the integrability of Lotka-Volterra equations: an update*, To appear in B. Toni (ed.), *Mathematical Sciences with Multidisciplinary Applications*, Springer Proceedings in Mathematics & Statistics **157**

A Geometric Approach for Invariant Algebraic Curves in 2D Lotka Volterra Systems II

C.J. Christopher[1], W.M.A. Hussein[2,3]

[1] *School of Computing, Electronics and Mathematics, Plymouth Univeristy, Plymouth, UK, c.christopher@plymouth.ac.uk*
[2] *School of Computing, Electronics and Mathematics, Plymouth University, Plymouth, UK, wuria.hussein@postgrad.plymouth.ac.uk*
[3] *Salahaddin-Hawler University, Kurdistan Region, Iraq, wuria.hussein@su.edu.krd*

In 2001, Moulin-Ollagnier [1, 2] classified all families of two dimensional Lotka-Volterra systems which have invariant algebraic curves. Twenty-five families of such curves were found using an essentially algebraic search. Our interest is to re-evaluate these families in terms of their geometric behavior. Although we are not able to provide a complete geometric proof of Moulin-Ollagnier's result, we are able to give geometric necessary conditions for the possible families of curves of low degree and, in some of these cases, can also prove the sufficiency of these conditions in purely geometric terms. The talk will be in two parts: the first will give the background and some of the tools used and the second will give more detailed examples. We will also show how this geometric understanding can be used to extend the classification of integrable critical points in Lotka Volterra systems started in [3]. This latter application is joint work with Zhaoxia Wang [4].

References

[1] J. Moulin-Ollagnier, *Liouvillian integration of the Lotka-Volterra system*, Qualitative Theory of Dynamical Systems **2**, 2, pp. 307-358 (2001).

[2] J. Moulin-Ollagnier, *Corrections and complements to Liouvillian integration of the Lotka-Volterra system*, Qualitative Theory of Dynamical Systems **5**, 2, pp. 275-284 (2004).

[3] C. Christopher and C. Rousseau, *Normalizable, integrable and linearizable saddle points in the Lotka-Volterra system*, Qualitative Theory of Dynamical Systems **5**, 1, pp. 11-61 (2004).

[4] C. Christopher, W.M.A. Hussein and Z. Wang, *On the integrability of Lotka-Volterra equations: an update*, To appear in B. Toni (ed.), *Mathematical Sciences with Multidisciplinary Applications*, Springer Proceedings in Mathematics & Statistics **157**

A Dynamical Systems Approach to Singularities of Ordinary Differential Equations

Werner M. Seiler[1]

[1] *Institut für Mathematik, Universität Kassel, Germany, seiler@mathematik.uni-kassel.de*

In this talk, we will discuss singularities of differential equations (as opposed to singularities of solutions of differential equations) using a geometric approach. A differential equation is considered as a submanifold of a jet bundle and a point on this submanifold is a singularity, if it is a critical point for the restricted projection to the base manifold. Thus one may consider this as a special case of the theory of singularities of smooth maps between manifolds [1].

An important geometric structure on a differential equation is its Vessiot distribution [2] and singularities can be characterised by changes in its properties. In the case of ordinary differential equations, the Vessiot distribution is generally one-dimensional and thus locally generated by a single vector field. At a regular singularity the distribution becomes vertical (but remains one-dimensional), whereas at an irregular singularity its dimension jumps. One can show that generically any vector field that generates the Vessiot distribution outside an irregular singularity vanishes when continued to the singularity [3].

In the talk we will show how the analysis of the local solution behaviour around an irregular singularity can thus be reduced to the analysis of a stationary point of an autonomous dynamical system. We will furthermore discuss the special case of a quasi-linear system (which is dominant in applications) [4]. Here we will first show that the Vessiot distribution becomes projectable and thus the problem can be considered at a lower order. Furthermore, we will show that this fact allows for genuine quasi-linear phenomena not present in general fully non-linear equations.

References

[1] M. Golubitsky, V. Guillemin, *Stable Mappings and Their Singularities*, Springer-Verlag, New York (1973).

[2] D. Fesser, W.M. Seiler *Existence and Construction of Vessiot Connections*, SIGMA **5**, 092 (2009).

[3] U. Kant, W.M. Seiler, *Singularities in the Geometric Theory of Differential Equations*, in *Dynamical Systems, Differential Equations and Applications (Proc. 8th AIMS Conference, Dresden 2010)*, Vol. 2, eds. W. Feng et al., AIMS, pp. 784–793, (2012).

[4] W.M. Seiler, *Singularities of Implicit Differential Equations and Static Bifurcations*, in *Computer Algebra in Scientific Computing – CASC 2013*, eds. V.P. Gerdt et al., Springer-Verlag, pp. 355–368, (2013)

Singular Initial Value Problems for Quasi-Linear Ordinary Differential Equations

Matthias Seiß[1]

[1] *Institut für Mathematik, Universität Kassel, Germany, mseiss@mathematik.uni-kassel.de*

In this talk, we will discuss the existence and non-uniqueness of solutions of intial value problems for quasi-linear ordinary differential equations where the initial condition corresponds to a singular point of the equation.
In the literature there are many publications (e.g. [2] and [3]), even monographs [1], where the authors solve this problem with analytic methods, such as fixed-point theorems or sub- and super-solutions, for quasi-linear differential equations of orders one and two. In this talk we will use for our analysis the differential geometric approach presented by Werner M. Seiler in *A Dynamical Systems Approach to Singularities of Ordinary Differential Equations*, that is, we will consider a quasi-linear differential equation as a submanifold of a jet bundle equipped with a geometric structure, the Vessiot distribution. Singular points on the differential equation are critical points for the restricted projection to the base manifold. They can be characterised by changes in the properties of the Vessiot distribution.
In the case of a quasi-linear differential equation, the Vessiot distribution is projectable to the next lower jet bundle and we will work there. In this situation, points where properties of the projected Vessiot distribution change will be called impasse points to distinguish them from singular points on the differential equation. For us a generalised solution will be an invariant one-dimensional submanifold with respect to a generator of the projected Vessiot distribution.
In this talk, we are interested in the behaviour of generalised solutions of a quasi-linear differential equation near an impasse point. More precisely, we will discuss the existence and non-uniqueness of generalised solutions starting at or going through such a point. We will place emphasis on impasse points where the projected Vessiot distribution vanishes, since they are stationary points of the corresponding dynamical system. We will apply methods from the theory of dynamical systems to examples of quasi-linear differential equations of orders one and two to analyse there the behaviour of their generalised solutions. In addition we will treat the special case of an autonomous second order quasi-linear differential equation.

References

[1] R.R. Agarwal, D. O'Regan, *Singular Differential and Integral Equations with Applications*, Kluwer, Dordrecht, 2003.

[2] Jianfeng Liang, *A singular initial value problem and self-similar solutions of a nonlinear dissipative wave equation*, Journal of Differential Equations, 246, pp. 819-844 (2009).

[3] Pavol Brunovsky, Ales Cerny, Michael Winkler, *A singular differential equation stemming from an optimal control problem in financial economics*, arXiv:1209.5027.

S7
Information Services for Mathematical Software, Models, and Research Data

Information services for mathematical research data

W. Sperber[1]

[1] *FIZ Karlsruhe, Berlin, Germany, wolfram@zentralblatt-math.org*

Publications are the classical means of mathematical information and communication containing also some classes of mathematical research data, especially models and objects But the advent of the computer has changed the situation. Typically, mathematical software is an own object not contained in publications. But the use of mathematical software becomes more and more important. Information services for mathematical software and other research data are challenging for some reasons:

- Mathematical software is written in a formal language and requires special data formats.
- Mathematical software is dynamic.
- Widely accepted standards for the description and content analysis, maintaining and archving of information about mathematical software are missing.

The talk discusses the spectrum of mathematical research data and a method to build information services for mathematical research data, the so-called publication-based approach. It seems to be that the publication-based approach is an effective means for the development of some information services for mathematical research data, especially directories and search engines. The concept bases on the fact that mathematical software is often accompanied by publications. This can be used to identify references to mathematical research data as well as to gain and evaluate information about mathematical research data via mathematical publications. The possibilities and limits of the publication-based approach are analyzed.

The swMATH service for mathematical software - state of the art and perspectives

Hagen Chrapary[1], Winfried Neun[2]

[1] *FIZ Karlsruhe/Zentralblatt MATH, Berlin, Germany, hagen@zentralblatt-math.org*
[2] *Zuse Institute Berlin (ZIB), Berlin, Germany, neun@zib.de*

The swMATH service is an open access portal for mathematical software and linked objects (benchmarks, data sets, languages, web services). It provides information on more than 13,000 items in all mathematical fields and lists nearly 125,000 scientific publications citing the software. We compare the swMATH information about Computer Algebra Software (CAS) with similar Web resources in symbolic computation, e.g. Wikipedia, SIGSAM or the German Computer Algebra Special Interest Group. The focus is on automatically generated information from our publication-based approach. As an example we present a software profile, which provides summarized information based on the Mathematical Subject Classification (MSC) tags of articles in the zbMATH database. An overview of open problems and next steps towards a better embedding of swMATH into scholarly communication will be given. We illustrate our concept with an online demonstration.

References

[1] swMATH: an information service for mathematical software, `http://www.swmath.org`.
[2] zbMATH: the first resource for mathematics, `https://zbmath.org`.
[3] Mathematical Subject Classification (MSC), `https://zbmath.org/classification/`.
[4] ACM Special Interest Group in Symbolic and Algebraic Manipulation, `http://www.sigsam.org/`.
[5] German Computer Algebra Special Interest Group, `http://www.fachgruppe-computeralgebra.de/`.
[6] Wikipedia CAS, `https://en.wikipedia.org/wiki/Computer_algebra_system`.

The SYMBOLICDATA Project – a Community Driven Project for the CA Community

H.-G. Gräbe

Leipzig University, Germany, graebe@informatik.uni-leipzig.de

1 Introduction

A central phenomenon of the emerging digital age is the increasing importance of a sustainably and reliably available *digital interconnection infrastructure* for many areas of every day life. This distinguishes the digital age from the computer age that focused on penetration of every day life with *compute power* rather than interconnectedness. With "ubiquitous computing" such a penetration with compute power reached a high level of saturation, but is in no way at its end as is demonstrated by the development of modern sensor and actor systems as "cyber-physical systems" and its applications within "industry 4.0".

During the last years the sensibility to the importance of investments also into a modern digital research infrastructure remarkably increased. It was continuously discussed on the "big" stage of research politics between different stakeholders, see e.g., [11, 12]. The disposition to invest into the development of an appropriate digital infrastructure heavily depends on the visibility of the demand, whereas the demand develops with the productiveness of the available infrastructure – a typical chicken-and-egg problem, that can only be addressed in the socio-technical context of a problem-aware community. Such a community should have a good understanding of the importance of the advancement of its own research infrastructure and the ability to set up a socio-communicative process to coordinate the development of its own demands *and* activities in the desired direction.

Digital infrastructures are not only well suited to exchange research data and make it publicly available, but also proved valuable as technical basis of "social networks" to promote such socio-communicative coordination processes. Nowadays in many cases different channels and means are used for these purposes, but it is due time to combine conceptually and also in practice both aspects of a research infrastructure.

With the advancement of the SYMBOLICDATA Project towards a Computer Algebra Social Network (CASN) we pursued such a concept in a specific context for several years. We started to investigate questions of intra- and intercommunity communication in correlation with practical aspects of the community driven development of a decentrally organized, distributed semantic-aware digital research

infrastructure within the specific research domain of *symbolic and algebraic computations* (CA) coarsely defined by the MSC 2010 classification code 68W30 – a medium sized scientific community, that splits into a number of subcommunities. These CA subcommunities are organized around special research topics and in many cases already managed to organize and consolidate their own intracommunity digital research infrastructures.

In our talk we address relevant questions, observations, and experience of our endeavor to develop and provide technical means to support the emergence of a digital research infrastructure on the intercommunity level. We discuss lessons to be learned from these activities and hurdles and obstructions to generalize intracommunity experience to an intercommunity level within the CA domain.

We propose to deploy a special RDF-based architecture of *CASN nodes* operated by different CA subcommunities and CA groups along the rules of the Linked Open Data Cloud [8]. To ensure interoperability, this should be accompanied by a strong social intercommunity communication process to develop a common *data architecture* of data models and its ontological standards of representation based on well established semantic web concepts and using standard semantic web technology.

2 The SYMBOLICDATA Project as Community Project

The allocation of resources for a sustainably available research infrastructure seems to be a great challenge in particular to smaller scientific communities. The SYMBOLICDATA Project witnesses the peaks and troughs of such efforts. It grew up from the Special Session on Benchmarking at the 1998 ISSAC conference in a situation where the research infrastructure built up within the PoSSo [10] and FRISCO [3] projects – the Polynomial Systems Database – was going to break down. After the end of the projects' fundings there was neither a commonly accepted process nor dedicated resources to keep the data in a reliable, concise, sustainably and digitally accessible way. Even within the ISSAC Special Session on Benchmarking the community could not agree upon a further roadmap to advance that matter.

At those times almost 20 years ago most of the nowadays well established concepts and standards for storage and representation of research data did not yet exist – even the first version of XML as a generic markup standard had to be accepted by the W3C. It was Olaf Bachmann and me who developed during 1999–2002 with strong support by the Singular group concepts, tools and data structures for a structured representation and storage of this data and prepared about 500 instances from *Polynomial Systems Solving* and *Geometry Theorem Proving* to be available within this research infrastructure, see [1].

The main conceptual goal was a nontechnical one – to develop a research infrastructure that is independent of (permanent) project funding but operates based on overheads of its users. This approach was inspired by the rich experience of the Open Culture movement "business models" to run infrastructures. During the last ten years with Open Access, Open Data and the emerging semantic web the general understanding of the importance of such community-based efforts to develop common research infrastructures matured. This development was accompanied with conceptual, technological and architectural standardization processes that had also impact on the development of concepts and data structures within the SYMBOLICDATA Project.

In 2009 we started to refactor the data along standard Semantic Web concepts based on the Resource Description Framework (RDF). With SYMBOLICDATA version 3 released in September 2013 we completed a redesign of the data along RDF based semantic technologies, set up a Virtuoso based RDF triple store and an SPARQL endpoint as Open Data services along Linked Data standards [8], and started both conceptual and practical work towards a semantic-aware Computer Algebra Social Network [5].

In March 2016 version 3.1 of the SYMBOLICDATA tools and data was released. On the level of research tools and data the new release contains new resource descriptions ("fingerprints" in the notion of [5]) of remotely available data on transitive groups (*Database for Number Fields* of Gunter Malle and Jürgen Klüners [7]) and polytopes (databases of Andreas Paffenholz [9] within the *polymake* project [4]), a recompiled and extended version of test sets from integer programming – work by Tim Römer (*normaliz* group [2]) – and an extended version of the *SDEval benchmarking environment* – work by Albert Heinle [6].

The main development is coordinated within the SYMBOLICDATA *Core Team* (Hans-Gert Gräbe, Ralf Hemmecke, Albert Heinle) with direct access to our public github account `https://github.com/symbolicdata`. We refer to the SYMBOLICDATA Wiki [13] for more details about the project and the new release.

3 The CA Community and its Subcommunities

During the last years the SYMBOLICDATA Project adjusted its focus to address more general technical and social aspects of a semantically enriched research infrastructure within the domain of Computer Algebra based on RDF for representation of intercommunity and relational information. Such a change of the focus had its impact on several earlier design decisions of the data store itself.

Enlarging the database of SYMBOLICDATA we gained the following experience:

- The CA community consists of several subcommunities with own concepts, notational conventions, semantic-aware tools and established communication structures.

  There is no need to duplicate such structures but to support the subcommunities to enrich semantically these communication processes.

- We provide structural metadata ("fingerprints" in the notion of [5]) of the different data sets at our central RDF store but not necessarily duplicate the data itself.

  Thus we rely on sustainably available research infrastructures of CA subcommunities and restrict our activities to a central search and filter service on the metadata level to find and identify data. This service is based on a generic semantic web concept, the SPARQL query language, and can be operated via our SPARQL endpoint.

- RDF is a useful and meanwhile well established standard for metadata and relational information, but there is no need and one cannot expect from CA subcommunities to give up established notational conventions in favor of RDF or XML markup for their primary sources.

4 About the CASN Architecture

The CASN subproject tries to embed aspects of the maintenance of the SYMBOLICDATA data store into a more general process of formation of a semantically enriched social network of academic communication within the CA community in the sense of a (social) "web of people".

A first roadmap towards such a CASN and our experimental setting was described in [5] and developed further during the last years. We try not to "reinvent the wheel" but to address step by step the already existing "CA memory" – a huge number of very loosely related web pages about conferences, meetings, working groups, projects, private and public repositories, private and public mailing lists etc. Hence the main focus towards CASN is to develop a framework based on modern semantic technologies for a decentralized network that increases the awareness of the different parts of that already existing "CA network".

We realized that this network itself is an "overlay network" that connects a greater number of research networks of individuals around special topics with own lightweight research infrastructures. It is an interesting challenge for semantic concepts to support the requirements of intercommunity communication to exchange semantic content on different levels and different levels of detail.

As a coarse architectural concept to establish such a network we propose

- to operate a central RDF store with SPARQL endpoint providing the full bandwidth of Linked Open Data services and
- to convert nodes of the "CA memory" into CASN nodes providing part of their data in structured RDF format for easy access and exchange.

SYMBOLICDATA version 3.1 is a first step in that direction since several data from the formerly separate CASN RDF store are now integrated within the SYMBOLICDATA main RDF store and the experimental setting of the semantic support of the website of the German Fachgruppe [14] was reorganized as a first CASN node.

References

[1] O. Bachmann, H.-G. Gräbe: The SymbolicData Project – Towards an Electronic Repository of Tools and Data for Benchmarks of Computer Algebra Software. Reports on Computer Algebra 27 (2000), Centre for Computer Algebra, University of Kaiserslautern.

[2] W. Bruns, B. Ichim, T. Römer, R. Sieg, C. Söger: Normaliz. Algorithms for Rational Cones and Affine Monoids. `https://www.normaliz.uni-osnabrueck.de`. [2016-03-08]

[3] FRISCO – A Framework for Integrated Symbolic/Numeric Computation. (1996–1999). `http://www.nag.co.uk/projects/FRISCO.html`. [2016-02-19]

[4] E. Gawrilow, M. Joswig: Polymake: a Framework for Analyzing Convex Polytopes. In: G. Kalai, G.M. Ziegler (eds.), Polytopes – Combinatorics and Computation (Oberwolfach, 1997), pp. 43–73, DMV Sem., 29, Birkhäuser, Basel (2000).

[5] H.-G. Gräbe, S. Johanning, A. Nareike: The SYMBOLICDATA Project – Towards a Computer Algebra Social Network. In: Workshop and Work in Progress Papers at CICM 2014, CEUR-WS.org, vol. 1186 (2014).

[6] A. Heinle, V. Levandovskyy: The SDEval Benchmarking Toolkit. ACM Communications in Computer Algebra, vol. 49.1, pp. 1–10 (2015).

[7] J. Klüners, G. Malle: A Database for Number Fields. `http://galoisdb.math.uni-paderborn.de/`. [2016-03-08]

[8] The Linked Open Data Cloud. `http://lod-cloud.net/`. [2016-05-20]

[9] A. Paffenholz: Polytope Database. `http://www.mathematik.tu-darmstadt.de/~paffenholz/data/`. [2016-03-08]

[10] The PoSSo Project. Polynomial Systems Solving – ESPRIT III BRA 6846. (1992–1995). `http://research.cs.ncl.ac.uk/cabernet/www.laas.research.ec.org/esp-syn/text/6846.html`. [2016-03-16]

[11] Research Infrastructures, including e-Infrastructures. `http://ec.europa.eu/programmes/horizon2020/en/h2020-section/research-infrastructures-including-e-infrastructures`. [2016-03-16]

[12] Strategy Report on Research Infrastructures. Roadmap 2016. Published by the European Strategy Forum for Research Infrastructures (ESFRI), Brüssel (2016). `http://www.esfri.eu/roadmap-2016`. [2016-03-16]

[13] The SYMBOLICDATA Project. `http://wiki.symbolicdata.org`. [2016-05-20]

[14] Website of the German Fachgruppe Computeralgebra. `http://www.fachgruppe-computeralgebra.de/`. [2016-03-06]

Benchmarks for and Quality Evaluation of CAS

Albert Heinle[1]

[1] *University of Waterloo, Waterloo, Ontario, Canada*

The symbolic computation community designs and implements algorithms on a regular basis, solving problems coming from a variety of topics. Quite often improvements on existing implementations are presented, and their advantages are illustrated with tables of computation timings.

The inputs chosen for these timings are usually either obtained by random generation, or by selection from examples in the literature. This is absolutely acceptable practice if an implementation for an algorithm is the only one available. However, it becomes hard to evaluate the quality of multiple implementations of the same algorithm, if every developer team presents the resource consumption of their program using individually chosen inputs.

In many sub-areas of the symbolic computation community, we are in the situation that we can pick from a great selection of implementations. Yet, there is no community-wide agreed-upon set of inputs, with which the performance of every new and existing implementation can be evaluated in a fair and independent way. Hence, the assessment of new software is currently difficult for reviewers and developers.

After having a unified set of inputs, the other great challenge is to find a way to create and verify the presented timings in a transparent and reproducible way.

Other communities have already introduced such benchmarking practice, and for industry-relevant software this is a must. For example, one of the most rigorous and well thought-through framework was developed by and for the Satisfiability community (SAT / SMT), namely StarExec[1].

Databases containing relevant examples can be found throughout our community. Hence, we are close to being able to establish a good benchmarking practice. We will discuss current challenges and identified needs of the computer algebra community, and present the benchmarking framework SymbolicData:SDEval[2].

[1] `https://www.starexec.org`

[2] `http://wiki.symbolicdata.org/SDEval`

S8
Algebraic and Algorithmic Aspects of Differential and Integral Operator Session

Algebraic Theory of Linear Partial Differential Algebraic Equations

Werner M. Seiler[1]

[1] *Institut für Mathematik, Universität Kassel, Germany, seiler@mathematik.uni-kassel.de*

We discuss general, i. e. also under- and overdetermined, systems of linear partial differential equations (sometimes also called linear partial differential algebraic equations) using algebraic techniques like Gröbner or involutive bases. The main emphasis is on the construction of formally well-posed initial value problems where for every choice of formal power series as initial data a unique formal power series solution exists. This problem is essentially equivalent to finding complementary combinatorial decompositions for monomial modules. In addition, we show how the theory of Gröbner bases for ideals of linear differential operators leads natural to index concepts that can be directly defined for systems of partial differential equations without the need to reduce first to ordinary differential algebraic equations (e. g. via semi-discretisations or integral transforms).

References

[1] W.M. Seiler, *Involution — The Formal Theory of Differential Equations and its Applications in Computer Algebra*, Springer-Verlag, Berlin/Heidelberg (2010)

[2] W.M. Seiler and E. Zerz, *Algebraic Theory of Linear Systems: A Survey*, in *Surveys in Differential-Algebraic Equations II*, Springer-Verlag, Berlin/Heidelberg, eds. A. Ilchman and T. Reis, pp. 287–333 (2015).

Desingularization of First Order Linear Difference Systems with Rational Function Coefficients

M. A. Barkatou[1], M. Jaroschek[2]

[1] *XLIM UMR 7252 , DMI, University of Limoges, CNRS, 123, Avenue Albert Thomas, 87060 Limoges, France, moulay.barkatou@unilim.fr*
[2] *Technische Universität Wien, Institut für Informationssysteme 184/4, Favoritenstraße 9-11, 1040 Wien, Austria, mjarosch@forsyte.at*

It is well known that for a first order system of linear difference equations with rational function coefficients, a solution that is holomorphic in some left half plane can be analytically continued to a meromorphic solution in the whole complex plane. The poles stem from the singularities of the rational function coefficients of the system. Just as for systems of differential equations, not all of these singularities necessarily lead to poles in a solution, as they might be what is called removable. In our work, we show how to detect and remove these singularities and further study the connection between poles of solutions, removable singularities and the extension of numerical sequences at these points.

Deciding Rational Solvability of First-Order Algebraic Ordinary Differential Equations

G. Grasegger[1], N.T. Vo[2], F. Winkler[2]

[1] *Austrian Academy of Sciences, RICAM, Linz, Austria, georg.grasegger@ricam.oeaw.ac.at*
[2] *RISC, J.Kepler University Linz, Austria, {tvongoc, franz.winkler}@risc.jku.at*

The question of determining general solutions of an algebraic ordinary differential equation (AODE) has a long history, dating back to the work of L. Fuchs and H. Poincaré. Rational general solutions have been investigated by Feng and Gao ([2]), Chen and Ma ([1]) and Ngô and Winkler ([7]). Consider $F(x,y,y')=0$, a first-order AODE, where F is an irreducible polynomial in three variables over an algebraically closed field K. Replacing y' by a new indeterminate z, we obtain an algebraic equation $F(x,y,z)=0$ which defines a plane algebraic curve $\mathscr{C} := \{(a,b) \in A^2(\overline{K(x)}) \,|\, F(x,a,b)=0\}$ over the field $\overline{K(x)}$ of algebraic functions. We call it the corresponding algebraic curve. A parametrization of $\mathscr{C}$ is a rational map $\mathscr{P} : A^1(\overline{K(x)}) \to \mathscr{C}$ such that the image of $\mathscr{P}$ is dense in $\mathscr{C}$ with respect to Zariski topology. If furthermore $\mathscr{P}$ is a birational equivalence, it is called a proper parametrization. It is well-known that exactly the curves of genus 0 are parametrizable. A parametrization is represented as a pair of rational functions, say $\mathscr{P} = (p_1(t), p_2(t))$, with coefficients in $\overline{K(x)}$. If the curve $\mathscr{C}$ is parametrizable, then it has a proper parametrization $\mathscr{P}$ whose coefficients lie in an algebraic extension field of $K(x)$ of degree at most 2 over $K(x)$. A parametrization is called optimal if its coefficients lie in an algebraic extension field of lowest algebraic extension degree. In [4, 8] we find algorithms for computing optimal parametrizations over the rational numbers Q as well as $Q(x)$. We have extended this optimal parametrization algorithm to work over $K(x)$, and we see that a rational curve defined over $K(x)$ can always be parametrized over $K(x)$.

A rational solution of the differential equation $F(x,y,y')=0$ is a rational function $y(x) \in K(x)$, such that $F(x,y(x),y'(x))=0$. A solution $y(x)$ of the AODE is called a strong rational general solution, if $y = y(x,c) \in K(x,c) \setminus K(x)$ where c is a transcendental constant over $K(x)$.

We show that if the differential equation $F(x,y,y')=0$ has a strong rational general solution, then its corresponding curve is of genus 0. Furthermore, if the corresponding algebraic curve of the differential equation $F(x,y,y')=0$ is of genus 0, and $\mathscr{P} = (p_1, p_2) \in K(x,t)^2$ is an optimal parametrization, then there is a one-to-one correspondence between strong rational general solutions of the differential equation $F(x,y,y')=0$ and strong rational general solutions of a quasi-linear associated AODE. Since the associated AODE is of first order and of first degree, we

know by Fuchs [3] that it admits a strong rational general solution only if it is a linear or a Riccati equation. A linear equation of order one can be solved easily by integration. For Riccati equations, we refer to a complete algorithm for finding all rational solutions provided by Kovacic [6]. Hence, a complete decision algorithm for the existence of a strong rational general solution of a first-order AODE can be given.

Example. (Example 1.537 in Kamke [5]) We consider the differential equation $F(x,y,y') = (xy'-y)^3 + x^6y' - 2x^5y = 0$. Its corresponding curve has a strong rational parametrization

$$\mathscr{P}(t) = \left(-\frac{t^3x^5 - t^2x^6 + (t-x)^3}{t^3x^5}, -\frac{2t^3x^5 - 2t^2x^6 + (t-x)^3}{t^3x^6} \right).$$

Hence, the associated differential equation with respect to $\mathscr{P}$ is $\omega' = \frac{1}{x^2}\omega(2\omega - x)$. This is a Riccati equation and we can determine a rational general solution $\omega(x) = \frac{x}{1+cx^2}$. Hence, the differential equation $F(x,y,y') = 0$ has the rational general solution $y(x) = cx(x+c^2)$.

References

[1] G. Chen and Y. Ma. Algorithmic reduction and rational general solutions of first order algebraic differential equations. In *Differential equations with symbolic computation*, pages 201–212. Birkhäuser, Basel, 2005.

[2] R. Feng and X.-S. Gao. Rational General Solutions of Algebraic Ordinary Differential Equations. In J. Gutierrez, editor, *Proceedings of the 2004 International Symposium on Symbolic and Algebraic Computation*, ISSAC '04, pages 155–162, New York, 2004. ACM.

[3] L. Fuchs. Über Differentialgleichungen, deren Integrale feste Verzweigungspunkte besitzen. *Sitzungsberichte der Königlich Preussischen Akademie der Wissenschaften*, 1884:699–710, 1884.

[4] E. Hillgarter and F. Winkler. Points on algebraic curves and the parametrization problem. In *Automated Deduction in Geometry*, Lecture Notes in Computer Science, pages 189–207, New York, 1997. Springer Berlin Heidelberg.

[5] E. Kamke. *Differentialgleichungen: Lösungsmethoden und Lösungen*. B. G. Teubner, Stuttgart, 1997.

[6] J. J. Kovacic. An algorithm for solving second order linear homogeneous differential equations. *Journal of Symbolic Computation*, 2:3–43, 1986.

[7] L. X. C. Ngô and F. Winkler. Rational general solutions of parametrizable AODEs. *Publicationes Mathematicae Debrecen*, 79(3–4):573–587, 2011.

[8] J. R. Sendra, F. Winkler, and S. Pérez-Díaz. *Rational Algebraic Curves, A Computer Algebra Approach*, volume 22 of *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin Heidelberg, 2008.

Difference-Differential Dimension Polynomials and their Invariants

Alexander Levin

The Catholic University of America, USA, levin@cua.edu

Let K be an inversive difference-differential field of zero characteristic with basic sets of derivations $\Delta = \{\delta_1, \dots, \delta_m\}$ and automorphisms $\sigma = \{\alpha_1, \dots, \alpha_n\}$ (any two mapping from the set $\Delta \cup \sigma$ commute). Let Θ and Γ denote the free commutative semigroup generated by Δ and free commutative group generated by σ, respectively. The *orders* of elements $\theta = \delta_1^{k_1} \dots \delta_m^{k_m} \in \Theta$ and $\gamma = \alpha_1^{l_1} \dots \alpha_n^{l_n} \in \Gamma$ are defined as

$$\text{ord}\, \theta = \sum_{i=1}^{m} k_i \text{ and } \text{ord}\, \gamma = \sum_{j=1}^{n} |l_j|,$$

respectively. Furthermore, for any $r \in \mathbb{N}$, we set

$$\Theta(r) = \{\theta \in \Theta \,|\, \text{ord}\, \theta \leq r\} \text{ and } \Gamma(r) = \{\gamma \in \Gamma \,|\, \text{ord}\, \gamma \leq r\}.$$

Let Λ be the semigroup of all power products $\lambda = \delta_1^{k_1} \dots \delta_m^{k_m} \alpha_1^{l_1} \dots \alpha_n^{l_n}$ ($k_i \in \mathbb{N}$, $l_j \in \mathbb{Z}$). We define the orders of λ with respect to the sets Δ and σ as $\text{ord}_\Delta \lambda = \sum_{i=1}^{m} k_i$ and $\text{ord}_\sigma \lambda = \sum_{j=1}^{n} |l_j|$, respectively, and set

$$\Lambda(r,s) = \{\lambda \in \Lambda \,|\, \text{ord}_\Delta \lambda \leq r, \text{ord}_\sigma \lambda \leq s\} \qquad (r,s \in \mathbb{N}).$$

In what follows, "difference" always means "inversive difference" (that is, we consider both positive and negative powers of the basic translations α_i). Furthermore, we will use prefixes Δ-, σ- and Δ-σ- instead of adjectives "differential", "difference" and "difference-differential" , respectively. If $\eta = \{\eta_1, \dots, \eta_p\}$ is a finite subset of a Δ-σ-field extension of K, we write $K\langle\eta\rangle$ for the Δ-σ-field extension of K generated by η (as a field, $K\langle\eta\rangle = K(\{\lambda(\eta_i) \,|\, \lambda \in \Lambda, 1 \leq i \leq p\})$). The differential (Δ-) and inversive difference (σ-) field extensions of K generated by the set η are denoted by $K\langle\eta\rangle_\Delta$ and $K\langle\eta\rangle_\sigma$, respectively.

With the above notation, as it is shown in [4], there exist polynomials $\chi^\Delta_{\eta|K}(t), \chi^\sigma_{\eta|K}(t) \in \mathbb{Q}[t]$ such that

$$\chi^\Delta_{\eta|K}(r) = \sigma\text{-tr.deg}_K K\langle\Theta(r)\eta\rangle_\sigma \text{ and } \chi^\Delta_{\eta|K}(r) = \Delta\text{-tr.deg}_K K\langle\Gamma(r)\eta\rangle_\Delta$$

for all sufficiently large $r \in \mathbb{N}$. (If M is a subset of Θ or Γ, then $M\eta$ denotes the set $\{\mu(\eta_i) \,|\, \mu \in M, 1 \leq i \leq p\}$.) Furthermore, it is proved in [1] that there exists a polynomial in two variables $\psi_{\eta|K}(t_1,t_2) \in \mathbb{Q}[t_1,t_2]$ such that

$$\psi_{\eta|K}(r,s) = \text{tr.deg}_K K(\{\lambda(\eta_i) \,|\, \text{ord}_\Delta \lambda \leq r, \text{ord}_\sigma \lambda \leq s, 1 \leq i \leq p\})$$

for all sufficiently large $r, s \in \mathbb{N}$.

These polynomials (called *dimension polynomials* of the Δ-σ-field extension $L = K\langle\eta\rangle$ associated with the system of Δ-σ-generators η), generally speaking, depend on the set η. However, they carry certain invariants that are independent of η and therefore characterize the extension L/K itself. In this talk we will describe these invariants in terms of differential, difference and difference-differential transcendence degrees and Krull-type dimension of field extensions. We will also discuss methods of computation of dimension polynomials and generalizations of the results on their invariants to the case of a difference-differential field extension with arbitrary partition of basic sets of derivations and translations. (The existence of the corresponding multivariate dimension polynomials was proved in [2] and [3, Section 4.2].)

References

[1] A. B. Levin. *Reduced Gröbner bases, free difference-differential modules and difference-differential dimension polynomials*. J. Symbolic Comput., 30 (2000), 357–382.

[2] A. B. Levin. *Gröbner bases with respect to several orderings and multivariable dimension polynomials*. J. Symbolic Comput., 42 (2007), 561–578.

[3] A. B. Levin. *Difference Algebra*. Springer, 2008.

[4] A. B. Levin, A. V. Mikhalev. *D*imension polynomials of filtered differential G-modules and extensions of differential G-fields. Contemp.Math., 131 (1992), Part 2, 469–489.

Thomas Decomposition and Nonlinear Control Systems

D. Robertz[1]

[1] *Centre for Mathematical Sciences, Plymouth University, 2-5 Kirkby Place, Drake Circus, Plymouth PL4 8AA, UK, daniel.robertz@plymouth.ac.uk*

This talk presents joint work with Markus Lange-Hegermann. We apply the Thomas decomposition technique to nonlinear control systems, in particular to the study of the dependence of the system behavior on parameters. Thomas' algorithm is a symbolic method which splits a given system of nonlinear partial differential equations into a finite family of so-called simple systems which are formally integrable and define a partition of the solution set of the original differential system. Different simple systems of a Thomas decomposition describe different structural behavior of the control system in general. We give a short introduction to the Thomas decomposition method and show how notions such as invertibility, observability and flat outputs can be studied. A Maple implementation of Thomas' algorithm is used to illustrate the techniques on explicit examples.

References

[1] T. Bächler, V. P. Gerdt, M. Lange-Hegermann and D. Robertz, *Algorithmic Thomas Decomposition of Algebraic and Differential Systems*, J. Symbolic Comput. **47**, 10, pp. 1233–1266 (2012).

[2] T. Bächler and M. Lange-Hegermann, `AlgebraicThomas` *and* `DifferentialThomas`*: Thomas decomposition of algebraic and differential systems*, freely available at `http://wwwb.math.rwth-aachen.de/thomasdecomposition`.

[3] G. Conte, C. H. Moog and A. M. Perdon, *Nonlinear control systems*, vol. 242 of Lecture Notes in Control and Information Sciences, Springer, London, 1999.

[4] S. Diop, *Elimination in control theory*, Math. Control Signals Systems **4**, 1, pp. 17–32 (1991).

[5] S. Diop, *Differential-algebraic decision methods and some applications to system theory*, Theoret. Comput. Sci. **98**, 1, pp. 137–161 (1992).

[6] M. Fliess and S. T. Glad, *An Algebraic Approach to Linear and Nonlinear Control*, in: H. L. Trentelman and J. C. Willems (eds.), *Essays on Control: Perspectives in the Theory and its Applications*, pp. 223–267, Birkhäuser, Boston, 1993.

[7] M. Fliess, J. Lévine, P. Martin and P. Rouchon, *Flatness and defect of non-linear systems: introductory theory and examples*, Internat. J. Control **61**, 6, pp. 1327–1361 (1995).

[8] V. P. Gerdt, *On decomposition of algebraic PDE systems into simple subsystems*, Acta Appl. Math. **101**, 1-3, pp. 39–51 (2008).

[9] M. Lange-Hegermann and D. Robertz, *Thomas decompositions of parametric nonlinear control systems*, in: Proceedings of the 5th Symposium on System Structure and Control, Grenoble, France, pp. 291–296, 2013.

[10] M. Lange-Hegermann and D. Robertz, *Thomas Decomposition and Nonlinear Control Systems*, submitted for publication.

[11] H. Nijmeijer and A. van der Schaft, *Nonlinear dynamical control systems*, Springer, New York, 1990.

[12] V. Levandovskyy and E. Zerz, *Obstructions to genericity in study of parametric problems in control theory*, in: H. Park and G. Regensburger (eds.), *Gröbner bases in control theory and signal processing*, vol. 3 of Radon Ser. Comput. Appl. Math., pp. 127–149. Walter de Gruyter, Berlin, 2007.

[13] J.-F. Pommaret, *Partial differential control theory*, vol. 530 of Mathematics and its Applications, Kluwer, Dordrecht, 2001.

[14] J.-F. Pommaret and A. Quadrat, *Formal obstructions to the controllability of partial differential control systems*, in: Proceedings of IMACS, Berlin, Germany, vol. 5, pp. 209–214, 1997.

[15] D. Robertz, *Formal Algorithmic Elimination for PDEs*, vol. 2121 of Lecture Notes in Mathematics, Springer, Cham, 2014.

[16] J. M. Thomas, *Differential Systems*, vol. XXI of American Mathematical Society Colloquium Publications, American Mathematical Society, New York, N. Y., 1937.

Polylogarithms at the multi-indices of non-positive integers

Gérard H. E. Duchamp[1], Hoang Ngoc Minh[2], Ngo Quoc Hoan[3]

[1] *Paris XIII University, 93430 Villetaneuse, France, gheduchamp@gmail.com*
[2] *Lille II University, 59024 Lille, France, Hoang.Ngocminh@lipn.univ-paris13.fr*
[3] *Paris XIII University, 93430 Villetaneuse, France, quochoan_ngo@yahoo.com.vn*

Abstract

We extend the definition and construct several bases for polylogarithms Li_T, where T are recognizable, by a finite state (multiplicity) automaton and of alphabet $X = \{x_0, x_1\}$[1]. The kernel of the "polylogarithmic map" $\mathrm{Li}_\bullet$ is also characterized and provides a rewriting process which terminates to a normal form. We mostly concentrate on the algebraic aspects of this extension.

As a matter of fact, the interest of rational series is twofold: algebraic and analytic. Firstly (from the algebraic point of view) they are closed under shuffle products and the shuffle exponential of letters (and their linear combinations, see the paragraph about the algebra "star of the plane") is precisely their Kleene star. On the other hand the growth of their coefficients is tame[2] [9, 23, 24] and, as such, their associated polylogarithms can be (in the domain $Dom(\mathrm{Li})$) rightfully computed [15, 19, 21, 22]. Doing this, we recover many functions (as the simple polynomials), forgotten in the straight algebra of polylogarithms. Let us, now, go into details, using the notations of [1, 26].

1. We denote $\mathbb{C}^{\mathrm{rat}}\langle\langle X\rangle\rangle$ the closure of $\mathbb{C}\langle X\rangle$ by rational operations $\{+, \mathtt{conc}, ^*\}$ [1]. This space is closed by shuffle product and, for any $a_0, a_1 \in \mathbb{C}$, one has

$$\begin{aligned}(a_0x_0 + a_1x_1)^* &= (a_0x_0)^* \sqcup\!\sqcup (a_1x_1)^* \\ \Delta_{\sqcup\!\sqcup}((a_0x_0 + a_1x_1)^*) &= (a_0x_0 + a_1x_1)^* \otimes (a_0x_0 + a_1x_1)^*.\end{aligned}$$

In here, we denote $S^* = \sum_{n\geq 0} S^n, \forall S \in \mathbb{C}\langle X\rangle$. By the Kleene-Schützenberger theorem, a power series S belongs to $\mathbb{C}^{\mathrm{rat}}\langle\langle X\rangle\rangle$ iff it is *recognizable* by an automaton admitting *a linear representation* (β, μ, γ) of dimension $n \geq 1$, with $\beta \in \mathscr{M}_{n,1}(\mathbb{C}), \gamma \in \mathscr{M}_{1,n}(\mathbb{C}), \mu : X^* \mapsto \mathscr{M}_{n,n}(\mathbb{C})$ (a multiplicative morphism). For any $w \in X^*$, one has $\langle S \mid w\rangle = \beta\mu(w)\gamma$ (see [1, 6]).

[1] The space of rational series considered here is $(\mathbb{C}\langle X\rangle \sqcup\!\sqcup \mathbb{C}^{\mathrm{rat}}\langle\langle x_0\rangle\rangle \sqcup\!\sqcup \mathbb{C}^{\mathrm{rat}}\langle\langle x_1\rangle\rangle, \sqcup\!\sqcup, 1_{X^*})$, it is a subspace of $Dom(\mathrm{Li})$.

[2] *i.e.* for such a rational series S over X, their exists a real $K > 0$ and a positive real morphism χ such that, for any word w over the monoid X^*, the coefficient $|\langle S \mid w\rangle|$ is majorated by $K \times \chi(w)$ [6, 9, 23, 24].

2. We consider also the differential forms $\omega_0(z) = z^{-1}dz$, $\omega_1(z) = (1-z)^{-1}dz$ and denote Ω the cleft plane $\mathbb{C}\setminus(]-\infty,0]\cup[1,+\infty[)$ and $\lambda(z)$ the rational fraction $z(1-z)^{-1}$ belonging to the differential ring $\mathscr{C} := \mathbb{C}[z,z^{-1},(1-z)^{-1}]$, endowed with the differential operator $\partial_z := d/dz$ and with the element $1_\Omega : \Omega \to \mathbb{C}$, as unit (*i.e.,* for any $z \in \Omega, 1_\Omega(z) = 1$).

In continuation of [7, 9], the principal object of the present work is the *polylogarithm* function, well defined for any r-uplet $(s_1,\ldots,s_r) \in \mathbb{C}^r, r \in \mathbb{N}_+$ and for any $z \in \mathbb{C}$ such that $|z| < 1$, as follows

$$\mathrm{Li}_{s_1,\ldots,s_r}(z) := \sum_{n_1>\ldots>n_r>0} \frac{z^{n_1}}{n_1^{s_1}\ldots n_r^{s_r}} \quad \text{and} \quad \frac{\mathrm{Li}_{s_1,\ldots,s_r}(z)}{1-z} = \sum_{N\geq 0} \mathrm{H}_{s_1,\ldots,s_r}(N)\, z^N,$$

where the arithmetic function $\mathrm{H}_{s_1,\ldots,s_r} : \mathbb{N} \to \mathbb{Q}$ is called *harmonic sum* and is expressed by $\mathrm{H}_{s_1,\ldots,s_r}(N) := \sum_{N\geq n_1>\ldots>n_r>0} \frac{1}{n_1^{s_1}\ldots n_r^{s_r}}$.

By analytic continuation [11, 27] and after a theorem by Abel, for any $r \geq 1$, if $(s_1,\ldots,s_r) \in \{(s_1,\ldots,s_r) \in \mathbb{C}^r | \forall m = 1,\ldots,r; \sum_{i=0}^m \Re(s_i) > m\}$, one obtains *polyzeta* values as follows

$$\zeta(s_1,\ldots,s_r) := \lim_{z\to 1} \mathrm{Li}_{s_1,\ldots,s_r}(z) = \lim_{N\to\infty} \mathrm{H}_{s_1,\ldots,s_r}(N).$$

This is no more valid in the divergent cases and requires the renormalization of the corresponding divergent polyzetas. It is already done for the case of polyzetas at positive multi-indices [3, 4, 5, 23] and it is done [10, 13, 25] and completed in [7, 9] for the case of non-positive multi-indices.

To study the polylogarithms at non- positive (negative) multi-indices, one relies on [7, 9] (resp. [18, 20]). Let $Y = \{y_k\}_{k\geq 0}$ and $Y_0 = \{y_0\} \sqcup Y$ be the alphabets.

1. the (one-to-one) correspondence between the multi-indices $(s_1,\ldots,s_r) \in \mathbb{Z}^r_{\leq 0}$ (resp. $\mathbb{N}^r_{\geq 1}$) and the words $y_{s_1}\ldots y_{s_r}$ (resp. $x_0^{s_1-1}x_1\ldots x_0^{s_r-1}x_1$) in Y_0^* (resp. $X^*x_1 + 1_{X^*}$),
2. indexing polylogarithms by words $y_{s_1}\ldots y_{s_r} \in Y_0^*$: $\mathrm{Li}^-_{y_{s_1}\ldots y_{s_r}} = \mathrm{Li}_{-s_1,\ldots,-s_r}$.

Moreover, one obtains the polylogarithms at positive indices as image by the following isomorphism of the shuffle algebra [18], $\mathrm{Li}_\bullet : (\mathbb{C}\langle X\rangle, \sqcup\!\sqcup, 1_{X^*}) \longrightarrow (\mathbb{C}\{\mathrm{Li}_w\}_{w\in X^*}, \times, 1_\Omega)$, such that[3],

$$x_0^n \longmapsto \log^n(z)/n!, \quad x_1^n \longmapsto \log^n((1-z)^{-1})/n!, \quad x_0^{s_1-1}x_1\ldots x_0^{s_r-1}x_1 \longmapsto \mathrm{Li}_{x_0^{s_1-1}x_1\ldots x_0^{s_r-1}x_1}.$$

Extending over the set of rational power series on non commutative variables when possible, see discussion after (1), as follows

$$\text{with} \qquad S \;=\; \sum_{n\geq 0} \langle S \mid x_0^n\rangle x_0^n + \sum_{k\geq 1} \sum_{w\in(x_0^*x_1)^k x_0^*} \langle S \mid w\rangle\, w,$$

[3] With the section chosen below, one has $x_0^n \longmapsto \Big(\log(z) - \log(z_0)\Big)^n/n!$.

$$\text{one defines} \qquad \mathrm{Li}_S(z) \;=\; \sum_{n\geq 0}\langle S \mid x_0^n\rangle \frac{\log^n(z)}{n!} + \sum_{k\geq 1}\sum_{w\in(x_0^*x_1)^k x_0^*}\langle S \mid w\rangle \,\mathrm{Li}_w\,. \qquad (1)$$

Some of these sums do not converge for the topology of compact convergence [4] and we will call $Dom(\mathrm{Li})$, the space of series for which $\langle |\mathrm{Li}|\,|\,|S|\rangle$ is convergent [5]. The morphism $\mathrm{Li}_\bullet$ is not injective, but $\{\mathrm{Li}_w\}_{w\in X^*}$ are still linearly independant over $\mathscr{C}$ [22, 23].

Example 1 *i.* $1_\Omega = \mathrm{Li}_{1_{X^*}} = \mathrm{Li}_{x_1^*-x_0^*\sqcup\!\sqcup x_1^*}$.

ii. $\lambda = \mathrm{Li}_{(x_0+x_1)^*} = \mathrm{Li}_{x_0^*\sqcup\!\sqcup x_1^*} = \mathrm{Li}_{x_1^*-1}$.

iii. $\mathscr{C} = \mathbb{C}[\mathrm{Li}_{x_0^*}, \mathrm{Li}_{(-x_0)^*}, \mathrm{Li}_{x_1^*}]$.

iv. $\mathscr{C}\{\mathrm{Li}_w\}_{w\in X^*} = \{\mathrm{Li}_S \,|\, S\in \mathbb{C}[x_0^*]\sqcup\!\sqcup \mathbb{C}[(-x_0)^*]\sqcup\!\sqcup \mathbb{C}[x_1^*]\sqcup\!\sqcup \mathbb{C}\langle X\rangle\}$.

Let us consider also the operators, acting on $\mathscr{C}\{\mathrm{Li}_w\}_{w\in X^*}$ [24]:

$$\partial_z = d/dz, \theta_0 = zd/dz, \theta_1 = (1-z)d/dz,$$
$$\forall f\in\mathscr{C}, \qquad \iota_0^{(z_0)}(f) = \int_{z_0}^z f(s)\omega_0(s) \quad \text{and} \quad \iota_1(f) = \int_0^z f(s)\omega_1(s).$$

Here, the operator $\iota_0^{(z_0)}$ is well-defined then one can check easily that [7, 9, 21, 22]

1. The subspace $\mathscr{C}\{\mathrm{Li}_w\}_{w\in X^*}$ is closed under the action of $\{\theta_0,\theta_1\}$ and $\{\iota_0,\iota_1\}$ [6].
2. The operators $\{\theta_0,\theta_1,\iota_0,\iota_1\}$ satisfy in particular,

$$\theta_1+\theta_0 = \big[\theta_1,\theta_0\big] = \partial_z \quad \text{and} \quad \forall k=0,1, \theta_k\iota_k = \mathrm{Id},$$
$$[\theta_0\iota_1, \theta_1\iota_0] = 0 \quad \text{and} \quad (\theta_0\iota_1)(\theta_1\iota_0) = (\theta_1\iota_0)(\theta_0\iota_1) = \mathrm{Id}.$$

3. $\theta_0\iota_1$ and $\theta_1\iota_0$ are scalar operators within $\mathscr{C}\{\mathrm{Li}_w\}_{w\in X^*}$, respectively with eigenvalues λ and $1/\lambda$, *i.e.* $(\theta_0\iota_1)f = \lambda f$, and $(\theta_1\iota_0)f = (1/\lambda)f$.
4. Let $w = y_{s_1}\ldots y_{s_r}\in Y^*$ (then $\pi_X(w) = x_0^{s_1-1}x_1\ldots x_0^{s_r-1}x_1$) and $u = y_{t_1}\ldots y_{t_r}\in Y_0^*$. The functions Li_w and Li_u^- satisfy

$$\mathrm{Li}_w = (\iota_0^{s_1-1}\iota_1\ldots\iota_0^{s_r-1}\iota_1)1_\Omega, \qquad \mathrm{Li}_u^- = (\theta_0^{t_1+1}\iota_1\ldots\theta_0^{t_r+1}\iota_1)1_\Omega,$$
$$\iota_0\,\mathrm{Li}_{\pi_X(w)} = \mathrm{Li}_{x_0\pi_X(w)}, \qquad \iota_1\,\mathrm{Li}_w = \mathrm{Li}_{x_1\pi_X(w)},$$
$$\theta_0\,\mathrm{Li}_{x_0\pi_X(w)} = \mathrm{Li}_{\pi_X(w)}, \qquad \theta_1\,\mathrm{Li}_{x_1\pi_X(w)} = \mathrm{Li}_{\pi_X(w)},$$
$$\theta_0\,\mathrm{Li}_{x_1\pi_X(w)} = \lambda\,\mathrm{Li}_{\pi_X(w)}, \qquad \theta_0\,\mathrm{Li}_{x_1\pi_X(w)} = \mathrm{Li}_{\pi_X(w)}/\lambda.$$

[4] For example, (1) gives a series $\langle Li \mid x_0^*x_1\rangle$ which is not convergent.

[5] we denote by $|T|$, the extension, term by term of the function $z\mapsto|z|$, i.e.,

$$|T| = \sum_{w\in X^*} |\langle T \mid w\rangle|\; w.$$

[6] Here, we state the identities for indifferently for $\iota_0 = \iota_0^{(z_0)}$ or the classic ι_0, see [7, 9, 14].

Here, we explain the whole project of extension of $\mathrm{Li}_\bullet$, study different aspects of it, in particular what is desired of $\iota_i, i = 0, 1$. The interesting problem in here is to study what is expected of the sections $\iota_i, i = 0, 1$. In fact, we will use this construction to extend $\mathrm{Li}_\bullet$ to $\mathscr{C}\{\mathrm{Li}_w\}_{w\in X^*}$ and, after that, we extend it to a much larger rational algebra.

References

[1] J. Berstel, C. Reutenauer, *Rational series and their languages*, Springer-Verlag, 1988.

[2] Bui V. C., Duchamp G. H. E., Hoang Ngoc Minh V., Tollu C., Ngo Q. H., *(Pure) transcendence bases in ϕ-deformed shuffle bialgebras*, arXiv:1507.01089v1 [cs.SC].

[3] Costermans C., Enjalbert J. Y., Hoang Ngoc Minh, *Algorithmic and combinatorial aspects of multiple harmonic sums,* Discrete Mathematic & Theoretical Computer Science Proceedings, 2005.

[4] Costermans C., Hoang Ngoc Minh, *Some Results à l'Abel Obtained by Use of Techniques à la Hopf*, "W. Global Integrability of Field Theories and Applications", Daresbury (UK), 1-3, 11/2006.

[5] Costermans C., Hoang Ngoc Minh, *Noncommutative algebra, multiple harmonic sums and applications in discrete probability*, J. of Sym. Comp. (2009), pp. 801–817.

[6] G. Duchamp, C. Reutenauer, Un critère de rationalité provenant de la géométrie non-commutative (à la mémoire de Schützenberger), Inventiones Mathematicae, 128, 613–622, (1997).

[7] Gérard H. E. Duchamp, Hoang Ngoc Minh, Ngo Quoc Hoan, *Harmonic sums and polylogarithms at negative multi - indices*, submitted to the JSC, 2015.

[8] Duchamp G. H. E., Tollu C., *Sweedler's duals and Schützenberger's calculus*, In K. Ebrahimi-Fard, M. Marcolli and W. van Suijlekom (eds), Combinatorics and Physics, p. 67–78, Amer. Math. Soc. (Contemporary Mathematics, vol. 539), 2011.

[9] Duchamp G. H. E. , Hoang Ngoc Minh, Penson K. A., Ngô Q. H., Simonnet P., *Mathematical renormalization in quantum electrodynamics via noncommutative generating series*, 2015.

[10] Furusho H., Komori Y., Matsumoto K., Tsumura H., *Desingularization of multiple zeta-functions of generalized Hurwitz-Lerch type*, 2014.

[11] Goncharov A. B., *Multiple polylogarithms and mixed Tate motives*, 2001.

[12] Guo L., Zhang B., *Differential Birkhoff decomposition and the renormalization of multiple zeta values*, J. Number Theory vol 128 (2008), 2318–2339.

[13] Guo L., Zhang B., *Renormalization of multiple zeta values*, J. Alg. 319 (2008): 3770–809.

[14] Hoang Ngoc Minh, *Evaluation Transform*, Theoretical Computer Sciences, 79, 1991, pp. 163–177.

[15] Hoang Ngoc Minh, *Summations of Polylogarithms via Evaluation Transform*, Math. & Computers in Simulations, 1336, pp 707–728, 1996.

[16] Hoang Ngoc Minh, *Fonctions génératrices polylogarithmiques d'ordre n et de paramètre t*. Discrete Math., 180, pp. 221–242, 1998.

[17] Hoang Ngoc Minh, M. Petitot, J. Van der Hoeven, *Polylogarithms and Shuffle Algebra*, FPSAC98, Toronto, Canada, Juin 1998.

[18] Hoang Ngoc Minh, Jacob G., Oussous N. E. , Petitot M., *Aspects combinatoires des polylogarithmes et des sommes d'Euler-Zagier*, J. SLC, B43e, (1998).

[19] Hoang Ngoc Minh, Jacob G., *Symbolic Integration of meromorphic differential equation via Dirichlet function*. Discrete Math., 210, pp. 87–116, 2000.

[20] Hoang Ngoc Minh & Petitot M., *Lyndon words, polylogarithmic functions and the Riemann ζ function*, Discrete Math., 217, 2000, pp. 273–292.

[21] Hoang Ngoc Minh, *Differential Galois groups and noncommutative generating series of polylogarithms*, in "Automata, Combinatorics and Geometry". 7th World Multi-conference on Systemics, Cybernetics and Informatics, Florida (2003)

[22] Hoang Ngoc Minh, *Finite polyzêtas, Poly-Bernoulli numbers, identities of polyzêtas and noncommutative rational power series*, Proceedings of 4^{th} I. C. W, pp. 232–250, 2003, Turku, Finland.

[23] Hoang Ngoc Minh, *Algebraic combinatoric aspects of asymptotic analysis of nonlinear dynamical system with singular inputs*, Acta Academiae Aboensis, Ser. B **67**(2), 117–126 (2007)

[24] Hoang Ngoc Minh, *On a conjecture by Pierre Cartier about a group of associators*, Acta Math. Vietnamica (2013), 38, Issue 3, pp. 339–398.

[25] Manchon D., Paycha S., *Nested sums of symbols and renormalised multiple zeta functions*, Int Math Res Notices (2010) 2010 (24): 4628–4697.

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

[27] Zhao J., *Analytic continuation of multiple zeta functions*, Proc. A. M. S. 128 (5): 1275–1283.

Symbolic Computation for Rankin-Cohen Differential Algebras. Klein curve as a case study.

Eleanor Farrington[1], Emma Previato[2]

[1] *Massachusetts Maritime Academy, Buzzards Bay, MA 02532 efarrington@maritime.edu*
[2] *Department of Mathematics and Statistics, Boston University, Boston, MA 02215 ep@bu.edu*

Rankin-Cohen algebras were defined by Zagier [Z], who reprised the role of differential operators in the theory of modular forms, central in the 19th century but "surprisingly little (...) in more modern investigations". In brief, for $f(\tau)$ and $g(\tau)$ two modular forms of weights k, l respectively, on some group $\Gamma \subset PSL(2,\mathbb{R})$, let D be the differential operator $\frac{1}{2\pi\imath}\frac{d}{d\tau}$, given the expansion of the modular forms in τ, where $\frac{1}{2\pi\imath}\frac{d}{d\tau} = q\frac{d}{dq}$, $q = e^{2\pi\imath\tau}$ as usual. The n-th Rankin-Cohen bracket (so named by Zagier, after R.A. Rankin who studied the derivations on modular forms and H. Cohen who gave examples) of f and g is the only bilinear differential operator of degree $2n$ that acts on the graded vector space of modular forms on Γ, and is defined as follows (denoting $D^r f$ by $f^{(r)}$ for a form f):

$$[f,g]_n(\tau) = \sum_{r+s=n} (-1)^r \binom{n-k+1}{s} \binom{n-l+1}{r} f^{(r)}(\tau) g^{(s)}(\tau).$$

Zagier pursues the study of the algebraic structure that this operation gives to the ring of modular forms viewed as a differential module, observing that it is "not clear how far we would have to go to get the first relation or how much further to ensure that all subsequent relations obtained would be consequences of ones already found". Instead of determining the relations, he proposes the abstract concept of a Rankin-Cohen differential algebra and gives a "partial structure theorem".

In this work, we propose to use Symbolic Computation to detect minimal sets of relations for the case study of $\Gamma(7)$, the modular group of the Klein curve, the only algebraic curve of genus three with the largest possible group of automorphisms, motivated by the first-named author's Ph.D. Thesis [Farr], which uses techniques that allow us to deal explicitly with certain modular forms.

We apply the theory of Gröbner bases (as in [EGÔP]) to control the weight of the relations, and then perform a search (implemented in *Maple* syntax) for complete, minimal sets ot relations weight-by-weight; in consequence, our results only reach a(ny) finite given weight, but these relations are of interest, given the large number of open problems that concern the Klein curve (more specifically stated below).

Then, in order to further exploit the power of computation, we propose to study Rankin-Cohen differential algebras over finite fields; indeed, when giving their abstract definition in [Z], "We will suppose the ground field K to be of characteristic 0 (in our examples it is usually $\mathbb{Q}$ or $\mathbb{C}$) although it is clear that the theory makes sense in any characterisitc or, for that matter, even if we work over $\mathbb{Z}$ rather than a field." Since our strategy is to reduce cusp forms modulo a prime p, we assume that p does not divide the level [CFW], therefore $p \neq 7$ throughout.

1 Wronskians

The problem of determining the set of Weierstrass points on curves of arithmetic interest, such as the Fermat curves $x^N + y^N + z^N = 0$ and the modular curves $X(N)$, remains unsolved for all but a few values of N.

Klein's curve, unique in genus three with maximum number of automorphisms, is an object of current interest, studied in one or the other of its several presentations. As a covering of $\mathbb{P}^1$, [FK1, VII.3], it is a Riemann surface M given by the algebraic equation

$$w^7 = z(z-1)^2.$$

The function z is ramified (of ramification number 7) at the points 0, 1 and ∞, and we set: $P_0 = z^{-1}(0), \quad P_1 = z^{-1}(1), \quad Q = z^{-1}(\infty)$, and consider the following divisors: $(z) = \dfrac{P_0^7}{Q^7}$, $(dz) = \dfrac{P_0^6 P_1^6}{Q^8}$, $(w) = \dfrac{P_0 P_1^2}{Q^3}$. Per this calculation, the differentials

$$\frac{dz}{w^3}, \quad (z-1)\frac{dz}{w^5}, \quad (z-1)\frac{dz}{w^6}$$

have divisors $P_0^3 Q, \quad P_0 P_1^3, \quad P_1 Q^3$, hence give a basis for $\Omega^1(M)$. Using this basis we can find an embedding of M in $\mathbb{P}^2$ [FK1, III.10]. In fact, if we set $w = -XY^{-1}, \quad z-1 = X^3 Y^{-2}$ we find that the projective equation for the algebraic curve M is the quartic: $X^3Y + Y^3Z + Z^3X = 0$.

We can immediately conclude from the divisors of the differentials that the points P_0, P_1 and Q are Weierstrass points of weight 1. We turn to the Wronskian of to finish the search for the Weierstrass points. We recall that, denoting $W(f_1, \ldots, f_g)$ the Wronskian determinant for a basis $f_1(z), \ldots, f_r(z)$ of the canonical linear system, $|K|$, with associated linear series $\mathscr{L}(K)$, over an algebraic curve X of genus $g \geq 2$, in a local coordinate z, the zeros of $W(f_1, \ldots, f_g)(dz)^{g(g+1)/2}$ are the Weierstrass points for the curve X, the multiplicities of the zeros being their Weierstrass weights [M, VII.4]. Using the function z above as a local coordinate, since we already took into account the points over 0, 1 and ∞ where it ramifies, we compute $W(z) = 3!(z^3 - 8z^2 + 5z + 1)/(z^8(z-1)^5)$ The polynomial

$p(z) = z^3 - 8z^2 + 5z + 1$ has three distinct real roots, each of which corresponds to 7 distinct points on M. Thus M has 24 Weierstrass points, each of weight one.

We now consider a second method for finding the ordinary Weierstrass points, as in [R]. When $X(\Gamma)$ is the modular curve $\Gamma\backslash\mathscr{H}^*$, for Γ a subgroup of finite index in $SL_2(\mathbb{Z})$ and $\mathscr{H}^*$ the upper half plane with the cusps of Γ adjoined, the set of weight-2 cusp forms for Γ, $S_2(\Gamma)$, is isomorphic to the set of holomorphic 1-forms for the Riemann surface. Thus to build a Wronskian for $\Gamma\backslash\mathscr{H}^*$ we may use a basis $f_1, f_2, \ldots, f_g$ for $S_2(\Gamma)$, the Wronskian $W(f_1, f_2, \ldots, f_g)$ being a modular form of weight $g(g+1)$ for Γ.

The Klein curve X is isomorphic to the modular curve $X(7)$, with $\Gamma = \Gamma(7)$. Since $\Gamma(7)$ is normal in $SL_2(\mathbb{Z})$, this Wronskian is a modular form for $SL_2(\mathbb{Z})$ itself, with character $\det\rho$, for ρ the natural representation of $SL_2(\mathbb{Z})$ on the space of cusp forms of weight 2 for Γ. The choice of basis only affects the Wronskian by a nonzero complex multiple, while we are only concerned about its zeros; to eliminate the dependence on the choice of basis entirely we may require that the first nonzero coefficient in the Fourier expansion of the Wronskian at the cusp at ∞ be 1. Thus we can talk about the Wronskian for $\Gamma\backslash\mathscr{H}^*$.

In general, if the ramification index of Γ in $SL_2(\mathbb{Z})$ is r at ∞, we can express the Fourier expansion of $W(z)$ at ∞ as

$$W(z) = \sum_{n \geq n_0} a_n e^{2\pi i n z/r}, \quad a_{n_0} = 1.$$

For the case of $X(7)$, $g = 3$, so $W(z)$ is a cusp form of weight 12. The character factors through $SL_2(\mathbb{Z})/\{\pm 1\}\Gamma(7)$, hence is trivial, thus $W(z)$ is a cusp form for $SL_2(\mathbb{Z})$ itself. The only possibility is that $W(z) = \Delta$, the "modular discriminant: $\Delta = (2\pi)^{12} q \prod_{r=1}^{\infty} (1-q^r)^{24}$. Since Δ is never zero on $\mathscr{H}$, we find that the Weierstrass points are the cusps.

The Wronskian for the pluricanonical series, $\mathscr{L}(nK)$, $n \geq 2$ (associated to $|nK|$) gives the higher-order Weierstrass points [FK1, III.5]. In the pluricanonical case, the Wronskian for a modular curve $X(\Gamma)$ is an automorphic form of weight $(2n-1)^2 g(g-1)/2$ [FK2, 3.1].

Using the model for $X(7)$ given by $w^7 = z(z-1)^2$, we have found bases for the pluricanonical series $\mathscr{L}(nK)$ for X. Indeed, we observed that for $2 \leq n \leq 5$, pairwise multiplication of the elements of our previously found basis for $\mathscr{L}(K)$ leads to exactly $\dim \mathscr{L}(nK) = (2n-1)(g-1) - 1$ independent differentials. For example for $n = 2$, pairwise multiplication of the basis elements of $\mathscr{L}(K)$ above led to

$$\{\frac{1}{w^6}, \frac{1}{wz(z-1)}, \frac{1}{zw^3}, \frac{1}{w^2 z(z-1)}, \frac{1}{w^4 z}, \frac{1}{w^5 z}\}.$$

To use these Wronskians in the Rankin-Cohen algebra, we must find their q-expansion: our strategy is to first identify them as automorphic forms constructed from theta constants [FK2, III.2]; then use classical identities to embed (as Klein did) the curve in $\mathbb{P}^2$ [FK2, III.8.4]; and lastly, use an algebraic map to convert $\mathbb{P}^2$-coordinates into the meromorphic functions w, z on the curve as the 7-sheeted cover; retracing our steps, we have written the pluricanonical Wronskians as classical automorphic forms, and can Fourier-expand them. As Zagier notes, a "canonical" Rankin-Cohen algebra can be generated by a form in degree four and a degree-2 differentiation; our Wronskians are of course of higher degree, but he also considers, for comparison, a homogeneous generator F of arbitrary degree, provided it is not a zero-divisor, so our case study is a legitimate example of his theory.

2 Finite Fields

Modular forms in positive characteristic (we are only considering reduction of coefficient modulo a prime p, not Katz' theory which has an algebro-geometric definition and may give rise to non-liftable forms, an unsettled issue) still present challenges, such as the structure of their Hecke algebra [BK]. The Hecke operator makes sense in characteristic p, but others do not exist in characteristic zero, particularly "multiplication by the Hasse invariant"; the "theta operator" ϑ is defined in characteristic zero, in fact it is precisely what we called D following [Z], where it "destroys modularity" [K], but in positive characteristic it raises the weight by $p+1$: this $\vartheta := q\frac{d}{dq}$ acts formally on the q expansion of the discriminant Δ and the Eisenstein series E_4, E_6, and these can be chosen as generators of the (graded) ring of modular forms. In the recent monograph [K], the author implements some such operations in computation, using both MAGMA and its open-source counterpart SAGE, primarily with the goal of computing Fourier coefficients.

We propose to use our case-study $\Gamma(7)$ and computation in characteristic $p \neq 7$ (over a finite field or its algebraic closure), not only to study the structure of Rankin-Cohen algebras, but also with the goal of computing "theta cycles": these are specific to positive characteristic, and arise as follows. The multiplication $f \mapsto Af$, where A is the Hasse invariant, in characteristic p raises the weight by $p-1$ and leaves the q-expansion unchanged: the smallest weight in which a form f appears is called its "filtration" $w(f)$. Since $w(\vartheta^p f) = w(\vartheta f)$, one can attach to any mod p modular form f a $(p-1)$-tuple of integers, $\big(w(\vartheta f), w(\vartheta^2 f), ..., w(\vartheta^{p-1} f)\big)$, and this is called its theta cycle. These were investigated by J. Tate and classified by N. Jochnowitz in her thesis: they have applications to estimates on the number of local components of Hecke algebras. We study the action of the Rankin-Cohen

brackets on theta cycles: this might give us an extra handle on the relations of Rankin-Cohen algebras in characterisitc p.

3 Conclusions

Our underlying theme is that the use of differential operators in the theory of modular forms, especially as regards their dual nature as algebro-geometric or number-theoretic objects, should be revived in the spirit of the nineteeth century and made powerful by means of symbolic computation. We use cusp forms over the Klein curve, obtain a relationship between the algebraic and modular aspects, and computationally obtain explicit identities for the little-known Rankin-Cohen differential (graded) algebras; in positive characteristic, even over finite fields, our case-study potentially aids the quest for the structure of the Hecke algebra. Further motivation for using the Klein curve is a computational study of its differential-Galois aspects (when viewed as an algebraic cover) [SU], which can be related to the algebraic Wronskians, and which we plan to relate to its cusp forms, particularly in positive characteristic since the previous work was carried out over the complex numbers.

References

[BK] J. Bellaïche and C. Khare, *Level 1 Hecke algebras of modular forms modulo p*, Compos. Math. 151 (2015), no. 3, 397-415.

[CFW] J.B. Conrey, D.W. Farmer and P.J. Wallace, *Factoring Hecke polynomials modulo a prime*, Pacific J. Math. 196 (2000), no. 1, 123-130.

[EGÔP] J.C. Eilbeck, J. Gibbons, Y. Ônishi and E. Previato, From equations of Jacobians or Kummer varieties to Coble hypersurfaces, Preprint 2016.

[FK1] H. Farkas and I. Kra, Riemann Surfaces, Springer-Verlag, New York, 1980.

[FK2] H. Farkas and I. Kra, Theta Constants, Riemann Surfaces and the Modular Group, 37, Graduate Studies in Mathematics, American Mathematical Society, Providence, R.I. 2001.

[Farr] E.S.A. Farrington, Aspects of Klein's Quartic Curve, Thesis (Ph.D.) Boston University. 2010. 172 pp. ISBN: 978-1124-05913-6 ProQuest LLC2010.

[K] Kilford, L. J. P. Modular forms. A classical and computational introduction. Imperial College Press, London, 2008.

[M] R. Miranda, Algebraic Curves and Riemann Surfaces, 5, Graduate Studies in Mathematics, American Mathematical Society, Providence, R.I. 1997.

[R] D.E. Rohrlich, *Some remarks on Weierstrass points*, in: Number theory related to Fermat's last theorem (Cambridge, MA, 1981), 71-78, Progr. Math., **26**, Birkhäuser, Boston, MA, 1982.

[SU] M.F. Singer and F. Ulmer, *On a third order differential equation whose differential Galois group is the simple group of* 168 *elements*, in: Applied algebra, algebraic algorithms and error-correcting codes (San Juan, PR, 1993), LNCS, Springer, Berlin, 316–324, 673, 1993.

[Z] D. Zagier, *Modular forms and differential operators*, in: K. G. Ramanathan memorial issue. Proc. Indian Acad. Sci. Math. Sci. 104 (1994), no. 1, 57-75.

Tensor reduction systems for operator algebras and normal forms

Jamal Hossein Poor, Clemens G. Raab, Georg Regensburger

RICAM, Austrian Academy of Sciences, Linz, Austria
{jamal.hossein.poor,clemens.raab,georg.regensburger}@ricam.oeaw.ac.at

Ore algebras are a well-established algebraic tool for an algorithmic treatment of many common cases, like differential and difference operators. However, integral operators cannot be constructed that way, for example. We use our two-level generalization [2] of Bergman's basis-free setting in tensor algebras [1] that allows for smaller reduction systems and tends to make computations more efficient. In this setting, we present a heuristic analog of Buchberger's algorithm for computer-assisted construction of Gröbner bases starting from basic identities of operators. We illustrate it and the package `TenReS` [3] using integro-differential operators with linear substitutions as example. These operator algebras have applications to delay equations [4] and address the univariate case of [5].

References

[1] G. Bergman, *The diamond lemma for ring theory*, Adv. in Math. **29**, pp. 178–218 (1978).

[2] J. Hossein Poor, C. G. Raab, and G. Regensburger, *Algorithmic operator algebras via normal forms for tensors*, in *Proceedings of ISSAC 2016*, ACM (2016). To appear.

[3] J. Hossein Poor, C. G. Raab, and G. Regensburger, *Normal forms for operators via Gröbner bases in tensor algebras*, in *Proceedings of ICMS 2016*, volume 9725 of *LNCS*, Springer (2016). To appear.

[4] A. Quadrat, *A constructive algebraic analysis approach to Artstein's reduction of linear time-delay systems*, IFAC-PapersOnLine **48**, pp. 209–214 (2015).

[5] M. Rosenkranz, X. Gao, and L. Guo, *An algebraic study of multivariable integration and linear substitution*, arXiv:1503.01694 [math.RA] (2015).

Generalized integro-differential algebra from an operator point of view

Clemens G. Raab[1], Georg Regensburger[2]

[1] *RICAM, Austrian Academy of Sciences, Linz, Austria, clemens.raab@ricam.oeaw.ac.at*
[2] *RICAM, Austrian Academy of Sciences, Linz, Austria, georg.regensburger@ricam.oeaw.ac.at*

Differential algebras with a right inverse of their derivation are a generalization of integro-differential algebras where the induced evaluation is not required to be multiplicative. Using our new two-level tensor setting for algebras of linear operators, we systematically rediscover identities, e.g. integration by parts, in these generalized integro-differential algebras. This is done by a completion process similar to Buchberger's algorithm starting just from the algebraic axioms. We also illustrate how other formulas, like the Taylor formula or variation of constants, can be proven in this operator framework.

References

[1] J. Hossein Poor, C. G. Raab, and G. Regensburger, *Algorithmic operator algebras via normal forms for tensors*, in *Proceedings of ISSAC 2016*, ACM (2016). To appear.

[2] J. Hossein Poor, C. G. Raab, and G. Regensburger, *Normal forms for operators via Gröbner bases in tensor algebras*, in *Proceedings of ICMS 2016*, volume 9725 of *LNCS*, Springer (2016). To appear.

Classical left regular left quotient ring of a ring and its semisimplicity criteria

V. V. Bavula

University of Sheffield, UK, v.bavula@sheffield.ac.uk

Let R be a ring, C and L be the set of regular and left regular elements of R ($C \subseteq L$). Goldie's Theorem is a semisimplicity criterion for the classical left quotient ring $Q_{l,cl}(R) := C^{-1}R$. Semisimplicity criteria are given for the classical left regular left quotient ring ${}'Q_{l,cl}(R) := L^{-1}R$. As a corollary, two new semisimplicity criteria for $Q_{l,cl}(R)$ are obtained (in the spirit of Goldie).

Computer Algebraic Analysis: Achievements, Perspectives and Directions

V. Levandovskyy[1]

[1] *Lehrstuhl B für Mathematik, RWTH Aachen University, Germany,*
viktor.levandovskyy@math.rwth-aachen.de

Computer Algebraic Analysis widely uses tools from ring and module theory, from homological algebra and from dimension theory by particularly emphasizing the algorithmic component of the computations and the role of implementation of algorithms in computer algebra systems. In the realm of systems of linear partial functional operators with polynomial coefficients, Gel'fand-Kirillov dimension, Ore localization with associated torsion and closure, and decomposition of modules such as equidimensional filtration and a decomposition, arising from the generalized factorizing Gröbner algorithm find numerous applications. On the other hand, many special functions, appearing as modules over mentioned algebras of operators, can be viewed as representation of modules in certain functional spaces.

The description of special functions in [1] is given over algebras of operators with rational coefficients in the arguments. We recognize those algebras as Ore localizations of algebras with polynomial coefficients and aim at the *augmented* description of special functions (obtained with the tools, described above), which is valid in a much broader context.

In the talks by J. Hoffmann, N. Kruff, J. Nüßle, C. Schilli (RWTH Aachen, Germany) and A. Heinle (University of Waterloo, Canada) many particular topics of the presented program and implementations in SINGULAR:PLURAL [2] will be discussed in details. In my talk I will outline the state of the art, summarize and present open questions.

References

[1] Milton Abramowitz and Irene Ann Stegun: *Handbook of Mathematical Functions*, `http://dlmf.nist.gov`.

[2] Greuel, G.-M. and Levandovskyy, V. and Motsak, A. and Schönemann, H., PLURAL. *A* SINGULAR *4.0 Subsystem for Computations with Non-commutative Polynomial Algebras*. Centre for Computer Algebra, TU Kaiserslautern, (2016). `http://www.singular.uni-kl.de`

The purity filtration of modules over Auslander regular rings

C. Schilli[1], V. Levandovskyy[2]

[1] *Lehrstuhl D für Mathematik, RWTH Aachen University, Germany,*
christian.schilli@math.rwth-aachen.de
[2] *Lehrstuhl B für Mathematik, RWTH Aachen University, Germany,*
viktor.levandovskyy@math.rwth-aachen.de

The purity filtration of modules is an important tool originating from homological algebra. It gives structural properties of a module (such as equidimensional submodules and their homological grades) and has numerous applications, e. g. in solving or simplifying systems of linear partial functional equations.
Based on the work [1], we will define the purity filtration, show some of its properties and give an algorithm, which allows us to compute the purity filtration of a finitely presented module over an Auslander regular ring. If the ground ring is also Cohen-Macaulay, the purity filtration gives additional insights on the structure of the module (concerning Gel'fand Kirillov dimension), which also will be pointed out. Finally, we will illustrate this theory with some examples, computed with our implementation [2] and give interpretations of the results.

References

[1] A. Quadrat, *Grade filtration of linear functional systems*, Acta ApplicandæMathematicæ127, 27–86, 2013.

[2] C. Schilli, V. Levandovskyy, *purityfiltration.lib*, a SINGULAR library, `https://github.com/Singular/Sources/blob/spielwiese/singular/lib/purityfiltration.lib`, 2012.

Computation of all Factorizations in Certain Non-Commutative Rings.

Albert Heinle[1], Viktor Levandovskyy[2]

[1] *University of Waterloo, Waterloo, Canada*
aheinle@uwaterloo.ca
[2] *RWTH Aachen University, Aachen, Germany*
levandov@math.rwth-aachen.de

There exist many classifications of commutative integral domains with respect to factorization properties of their elements. Anderson et al. [AA92, AAZ90, AM96, And97] have coined certain terminology like finite factorization domain (FFD), half factorization domain (HFD), idf-domain and bi-factorization domain (BFD). Furthermore, they studied the connection between all these different types of domains with respect to implication. A recent paper [BS15] generalizes these notions to non-commutative rings, with applications to maximal orders in central simple algebras and the semigroup of non zero-divisors of the ring of $n \times n$ upper triangular matrices over a commutative domain. No algorithm for factorization has been proposed.

We study noncommutative domains with a view towards algorithms for factorizing concrete elements. In a recent publication [BHL14], a generalization of the term finite factorization domain, which applies to non-commutative rings, has been established. Namely, we consider factorizations up to multiplication with central units of the algebra. Necessary conditions on a given ring to be an FFD have also been formulated, leading to the result that among many other, the ubiquitous G-algebras (which are Noetherian domains) are FFDs. As a consequence, the problem formulation "find all distinct factorizations of an element in a G-algebra" becomes viable, since the output is expected to be finite.

An algorithm that finds all possible factorizations for an element in a G-algebra $\mathscr{G}$ with minor assumptions on the underlying field K has been established [HL16]. With this, one is able to generalize other algorithms, which were exclusively used for commuatative rings before. An example is the "Factorized Gröbner Basis" algorithm. However, the structure of the output of this algorithm in the non-commutative case has no direct interpretation as in the commutative case. We conjecture a strong connection to a decomposition of a solution space, when viewing elements in G-algebras as operator equations.

Our presentation will serve as an introduction into non-commutative finite factorization domains, provide an overview of the status quo of the factorization problem for G-algebras and its applications, and finishes with a vision on future ex-

ploration possibilities in the area of characterizing factorization properties in non-commutative integral domains.

References

[AA92] D.D. Anderson and David F Anderson. Elasticity of factorizations in integral domains. *Journal of pure and applied algebra*, 80(3):217–235, 1992.

[AAZ90] D.D. Anderson, David F. Anderson, and Muhammad Zafrullah. Factorization in integral domains. *Journal of pure and applied algebra*, 69(1):1–19, 1990.

[AM96] D. Anderson and Bernadette Mullins. Finite factorization domains. *Proceedings of the American Mathematical Society*, 124(2):389–396, 1996.

[And97] D. Anderson. *Factorization in integral domains*, volume 189. CRC Press, 1997.

[BS15] N.R. Baeth and D. Smertnig. Factorization theory: From commutative to noncommutative settings. *Journal of Algebra 441 (2015): 475-551*, 2015.

[BHL14] J. P. Bell, A. Heinle, and V. Levandovskyy. On noncommutative finite factorization domains. *To Appear in the Transactions of the American Mathematical Society; arXiv preprint arXiv:1410.6178*, 2014.

[HL16] A. Heinle, and V. Levandovskyy. A Factorization Algorithm for G-Algebras and Applications. *To Appear in the Proceedings of the "41st International Symposium on Symbolic and Algebraic Computation" (ISSAC'16)*, 2016.

Ore localization, associated torsion and algorithms

J. Hoffmann[1], V. Levandovskyy[2]

[1] *Lehrstul D für Mathematik, RWTH Aachen University, Germany,*
Johannes.Hoffmann@math.rwth-aachen.de
[2] *Lehrstul B für Mathematik, RWTH Aachen University, Germany,*
Viktor.Levandovskyy@math.rwth-aachen.de

Localizing a commutative ring at a multiplicatively closed subset is an important and well-understood tool in the study of commutative rings. For non-commutative domains, the concept of Ore localization at (left) Ore sets introduced by Øystein Ore ([1]) is a generalization that retains most of the properties of classical localization. Its most prominent application in the context of algebras of operators is the formalism of passing from polynomial to rational coefficients.

Building on previous results in the commutative setting well-known to Zariski and Samuel ([3]), we present a new canonical form for Ore sets that gives full insight into the structure of the associated localization and its units.

As a further application of Ore sets we introduce the concept of local torsion of modules over (non-commutative) domains, which results in a finer description of the torsion structure of a module.

In the case of finitely presented modules, local torsion is closely related to S-closure, i. e. the closure of submodules of free modules with respect to an Ore set, which is an instance of a more general construction that also encompasses the canonical form for Ore sets above.

Furthermore, we show a connection between S-closure and contraction of ideals in the localization to the unlocalized ring. There are several algorithmic approaches to the latter, most notably Weyl closure ([2]). We expand the algorithmic toolbox by a variation of a commutative algorithm that computes S-closure in a restricted setting which is of importance in the theory of D-modules.

References

[1] Øystein Ore, *Linear Equations in Non-Commutative Fields*, *Annals of Mathematics* 32 (3), 463–477, 1931.

[2] Harrison Tsai, *Algorithms for algebraic analysis*, PhD thesis, University of California at Berkeley, 2000.

[3] Oscar Zariski and Pierre Samuel, *Commutative Algebra Volume I*, Springer, 2nd ed., 1975.

Local Closure of Ore Algebras

J. Nüßle[1]

[1] *Lehrstuhl D für Mathematik, RWTH Aachen, Germany, nuessle@math.rwth-aachen.de*

Let K be a field, $K[x] = K[x_1, \ldots, x_n]$ the polynomial ring in n variables and $R := K[x][\partial; \mathrm{id}, \delta]$ an Ore extension of $K[x]$ with a derivation δ. This is an algebraic model for linear ODEs with the x_i taking the role of coefficient functions and δ modelling the derivative of those functions. Here the elements and ideals in R represent ODEs and systems of ODEs respectively. In this setting the contraction ideal

$$\mathrm{Cont}(I) := (K[x] \setminus \{0\})^{-1} I \cap R$$

for an ideal $I \subseteq R$ is the largest ideal in R that has the same solutions as I (on a suitably chosen open subset of the complex plane). The problem of computing the contraction ideal for a given ideal I has been solved e.g. in the Weyl algebra (see [1]) under the name of Weyl closure, but the general case remains unsolved.

If we restrict ourselves to principal ideals $\langle f \rangle \subseteq R$ it is enough to consider the local closure

$$\mathrm{Cl}_p(f) := \{p^{-k}\} \langle f \rangle \cap R$$

at the leading ∂-coefficient p of f. This relates to the problem of desingularization of differential operators, which has for example been considered (for $K[x] = K[x_1]$) by [2] or for a fixed maximal degree of the desingularizing operator by [3].

We will present an approach that can be used in the general case to compute all elements $h \in R$ such that $\frac{1}{p} hf \in R$ for a given $p \in K[x]$, i.e. all desingularizing operators that have degree 1 in $\frac{1}{p}$. Such h have some significance as $\mathrm{Cl}_p(f)$ is strictly larger than $\langle f \rangle$ if and only if the set of all $h \in R$ with $\frac{1}{p} hf \in R$ is strictly larger than pR. This means that we can test whether p is removable from f. Furthermore if p is removable from f there is always a p-removing operator of minimal degree in ∂ that has the form $\frac{1}{p} h$.

References

[1] H. Tsai, *Weyl closure of a linear differential operator*, Journal of Symbolic Computation, pp. 747-775 (2000).

[2] Y. Zhang, *Contraction of Ore Ideals with Applications*, The 41st International Symposium an Symbolic and Algebraic Computation, Waterloo, Canada, July 19-22, 2016.

[3] S. Chen, M. Kauers, M. Singer, *Desingularization of Ore operators*, Journal of Symbolic Computation, pp. 617-626 (Mai-June 2016).

Ore localization with applications in D-module theory

N. Kruff[1], V. Levandovskyy[2]

[1] *Lehrstuhl A für Mathematik, RWTH Aachen University, Germany, niclas.kruff@matha.rwth-aachen.de*

[2] *Lehrstuhl B für Mathematik, RWTH Aachen University, Germany, viktor.levandovskyy@math.rwth-aachen.de*

The global and local Bernstein-Sato polynomial of a given multivariate polynomial $f \in K[x_1, \ldots, x_n]$ where K is of characteristic zero, plays an important role in D-module theory and in singularity theory, to name a few. We are interested in computing the local Bernstein-Sato polynomial of a given polynomial at a given point $p \in K^n$. Although several algorithms for its computation are already known, we will present a new algorithm that uses Ore localizations. Theoretically, our algorithm needs to employ product localizations. However, we prove that it suffices to work in another localization which is algorithmically easier to handle. Finally, we provide an algorithmic approach to compute the local Bernstein-Sato polynomial at a point, given via algebraic but non-rational coordinates. Applying this algorithm, it is possible to compute local Bernstein-Sato polynomials using symmetry arguments.

S9
Automated Theorem Proving in Dynamic Geometry: Current Achievements

Intelligent Geometry + Dynamic Geometry

Pedro Quaresma[1]

[1] *CISUC/Department of Mathematics, University of Coimbra, Portugal, pedro@mat.uc.pt*

The pursue of an "Intelligent and Dynamic Geometry Book" should involve the study of how current developing methodologies and technologies of mathematical (e.g. geometry) knowledge representation, management, and discovery can be incorporated effectively into the education of the future.

Just as Doron Zeilberger pointed out in the *Plane Geometry: An Elementary Textbook By Shalosh B. Ekhad (Circa 2050)*,[1] a geometry book from the future should be a computer program, in which all the theorems can be automatically discovered (and of course proved) by computer and beautiful illustrations can be automatically generated and dynamically modified. Such a prospect motivates studies on how to represent and manage digitised geometric knowledge on computer.

The geometry book of the future should be adaptive, correct, collaborative, visual and intelligent. Adaptive because the contents would adapt to the curriculum and reader. Correctness of the proofs would be ensured by computer checking. It will allow collaborative work an its contents would be collaboratively formed using a knowledge base open to contributions. Statements and proofs should be enlighted by dynamic geometry sketches and diagrams. The book will be intelligent, the reader can ask closed or open questions, and can ask for proof hints. The book would also provide interactive exercises with automatic correction.

Such a blended-learning Cloud platform, freely available in all standard computational platforms and devices, collaborative, adaptive to each and every user's profiles, would bring together a whole new generation of mathematical tools with impact in all levels of education.

To realise such book we must build a network of experts, increasing the connections between several research communities, such as: *mathematical knowledge management*; *computer theorem proving and discovery*; *education*, aggregating expertise in areas such as *Proofs in a Learning Context*; *Interfaces & Searching*; *Tools Integration*; *Learning Environments in the Cloud*.

[1] `http://www.math.rutgers.edu/~zeilberg/GT.html`

sketchometry: a sketching tool for geometry

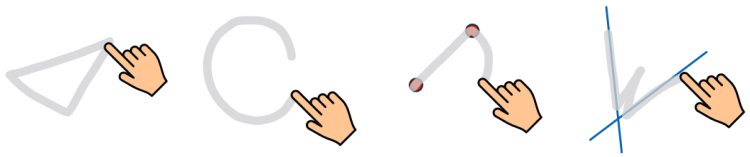
A. Wassermann[1]

[1] *Department of Mathematics, University of Bayreuth, 95440 Bayreuth, Germany, alfred.wassermann@uni-bayreuth.de*

sketchometry [1] is a free interactive geometry system with a focus on (but not restricted to) touch devices. The main distinctive feature of sketchometry in comparison with other interactive geometry systems is its ability to recognize sketches by the user. These strokes are converted into geometric objects.

Internally, *sketchometry* is based on *JessieCode* and *JSXGraph* [2,3]. *JSXGraph* is a comprehensive library for interactive geometry in the web browser, *JessieCode* [4] is a special purpose programming language for handling *JSXGraph* objects. It has been introduced to simplify the input of geometric constructions and for security reasons. Both projects are maintained by the developers of *sketchometry*.

In the talk, we will explain how the innovative user interaction of *sketchometry* is realized and give an overview how these three systems are used with requiring varying levels of sophistication.



References

[1] `http://sketchometry.org`

[2] M. Ehmann, C. Miller and A. Wassermann *Dynamic Mathematics with GEONE$_X$T – New Concepts*, 4th European Workshop on Mathematical & Scientific e-Contents, Trondheim 2008.

[3] `http://jsxgraph.org`

[4] `http://bin.sketchometry.org`

A constructive approach to the cuadrics of revolution and their equations using the DGS *GeoGebra*

E. Roanes-Lozano[1]

[1] *Instituto de Matemática Interdisciplinar (IMI) & Depto. de Álgebra, Universidad Complutense de Madrid, Spain, eroanes@mat.ucm.es*

Many authors have used different approaches to conics using dynamic geometry systems (DGS). The easiest one would be to introduce the equations and produce a plot. Moreover, the DGS *GeoGebra* [1] directly provides tools (with an icon in the *ToolBar*) that constructs the conic:

- given five points on it,
- given either the two foci and a point on the conic or the focus and the directrix of the conic (depending on which conic is considered).

But the prettiest approach is possibly the constructive one that uses properties of the conics to draw them (such as the gardener's method to draw ellipses). This method also allows the user to obtain automatically the equation of the conic from the given elements (given, for instance, in the case of the ellipse, the coordinates of the foci and the sum of distances to the foci).

The arrival of 3D DGS such as *Calques 3D* [2] or *GeoGebra 5* allows to extend the constructive methods mentioned above to cuadrics of revolution, substituting circumferences by spheres and lines by planes. Although more complex and laborious than in the 2D case, they allow to obtain both plots and equations of ellipsoids of revolution, paraboloids of revolution and hyperboloids of revolution. The elimination step requires of the internal use of effective algebraic methods that are hidden to the end user.

We believe that automatically obtaining the equations of these simple cuadrics as suggested could be eye-catching and motivating for students at their first encounter with this kind of surfaces.

References

[1] `https://www.geogebra.org/wiki/en/Manual`

[2] E. Roanes-Lozano, N. van Labeke and E. Roanes-Macías, *Connecting the 3D DGS Calques3D with the CAS Maple*, Math. Comp. Simul. **80**, 6, pp. 1153–1176 (2010). DOI: http://dx.doi.org/doi:10.1016/j.matcom.2009.09.008

Managing the constraints of technology for an automated study of envelopes

Th. Dana-Picard[1], N. Zehavi[2]

[1] *Jerusalem College of Technology, ndp@jct.ac.il*

[2] *Weizmann Institute of Science, nurit.zehavi10@gmail.com*

1 Introduction

We propose a short survey of issues we had to deal with when studying various questions in Differential Geometry using different Information and Communication Technologies (ICT). The mathematical topic we address here is envelopes of parameterized families of curves or surfaces. We met similar constraints for other items, such as isoptic curves of a plane curve (see [2]). As far as possible, and for the sake of simplicity, we give 2D examples when 3D occurrences are similar. More details will be given during the oral presentation.

The study of parametric families of curves and surfaces (in what follows, we will call them varieties) in 2D and 3D spaces and their (possible) envelopes has a great interest in mathematics and its applications: Geometrical Optics and Theory of Singularities, robotics and kinematics, rigid motion in 2-space and in 3-space, collision avoidance, soil depollution, etc. In a recent work [3], we showed how envelopes can be studied with paper-and-pencil together with both a Computer Algebra System (CAS) and a Dynamical Geometry System (DGS). All the ICTs have their own constraints (see [6] and [1]), and we had to deal with some of them. In our talk, we will present constraints appearing when studying envelopes, using both a CAS and a DGS.

Our main goal is the study 1-parameter families of curves in 2D space (resp. surfaces in 3D space); we will call them varieties. They may have an implicit presentation, of the form $f(x,y,t) = 0$ (resp. $f(x,y,z,t) = 0$), where f is a function of 3 (resp. 4 variables), x,y (resp. x,y,z) are the coordinate system and t is a real parameter. A variety may have also a parametric presentation, in which the coordinates x,y (resp. x,y,z) are functions of one real parameter (for curves) and 2 parameters (for surfaces).

2 Visualization problems

First we describe general visualizations problems appearing both in 2D and in 3D. If the variety is given by a rational parametrization, the equations may be trans-

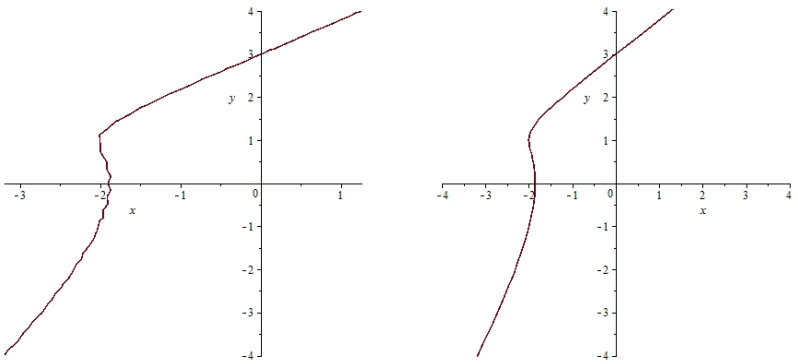
formed into polynomial equations, then Gröbner bases algorithms provide the required implicitization. For example, let $\mathscr{C}$ be the plane curve given by the following presentation:

$$x = t^3 + t^2 - 2$$
$$y = t^3 + t + 1$$

Here are some rows of Maple code for our purpose. First we transform the given parametrization of $\mathscr{C}$ into polynomials and consider them as generating an ideal $J = < x - t^3 - t^2 + 2, y - t^3 - t - 1 >$ in $R[x,y,t]$. Then using an elimination order, we compute a polynomial defining the curve $\mathscr{C}$ by an implicit equation.

```
> restart; with(plots); with(PolynomialIdeals);
> F1 := x-t^3-t^2+2; F2 := y-t^3-t-1;
> J := `<,>`(F1, F2);
> JE := EliminationIdeal(J, {x, y});
```

Using the **implicitplot** command, we obtain Figure 1 (a), and with parametric plot we obtain Figure 1 (b); the difference in quality is evident. In both cases, we used the standard number of points of the command (of course, increasing the number of computed points improves the plot quality).



(a) Implicit Plot (b) Parametric Plot

Figure 1: Two plots of the same curve

This inaccuracy may be even greater when dealing with curves and surfaces in 3D space, as we will see in the next example. Consider the unit sphere, which has

implicit equation $x^2+y^2+z^2=1$, and a parametric representation is given by

$$\begin{aligned} x &= \cos u \sin v \\ y &= \sin u \sin v \\ z &= \cos v \end{aligned} \tag{1}$$

where u and v are real parameters.

Consider Figure 2, it shows two plots of the unit sphere. Plot (a) has been obtained using an implicit representation, plot (b) using a parametric presentation. The difference in quality is evident. Increasing the number of cells of the mesh will not improve the visual effect of the implicit plot; the display will appear more black.

(a) Implicit Plot (b) Parametric Plot

Figure 2: Two plots of the unit sphere

The parametrization we used for the unit sphere is trigonometric. This variety has also rational parameterizations, for example:

$$\begin{aligned} x &= \frac{2v(1-u^2)}{(1+u^2)(1+v^2)} \\ y &= \frac{4uv}{(1+u^2)(1+v^2)} \\ z &= \frac{1-v^2}{1+v^2} \end{aligned} \quad , \tag{2}$$

where u and v are real parameters. Both parameterizations provide the same plot quality.

Equations 2 may be transformed into polynomial equations, then Gröbner base code will provide an implicit equation for the sphere. The algorithms which are used are clearly irrelevant for the trigonometric parametrization 1. Automatic derivation of an implicit equation is harder in this case.

Switching between a non rational parametrization and a rational one, and switching between parametric and implicit representations are a non trivial issue. In order to address this last question, algorithms have been developed for approximate implicitization (see [4] and [5]).

3 Automated study of envelopes

Let be given a family of plane curves by an equation of the form $f(x,y,t) = 0$, where t is a real parameter. An envelope of the family, if it exists, is a curve tangent to every curve in the family. It can be shown (see [3]) that this envelope is the solution set of the system of equations

$$\begin{cases} f(x,y,t) & = 0 \\ \frac{\partial f}{\partial t} f(x,y,t) & = 0 \end{cases}. \tag{3}$$

A first approach with a DGS (we used GeoGebra) yields an experimental study of the possible envelope. For example, Figure 3 shows the experimental study of the family of circles of radius 1.5, centered on the parabola whose equation is $y = x^2$.

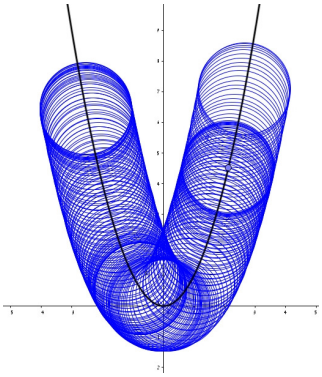


Figure 3: Family of circles centered on a parabola

The plot has been performed drawing one circle, then using the mouse to move the center along the parabola (with the **Trace On** option). The circles are not uniformally dispatched, the "gaps" being function of the speed of hand motion with the mouse. Anyway, two envelope components appear: the external one seems smooth, the internal one seems to have cusps and a double point. The same construction may have been performed using the slider bar. In this case, the circles are more uniformly dispatched. Nevertheless, even by that way, the plot may not show exactly what we expect; see the nephroid in [3]. Figure 3 shows a dynamical

construction, leading to the conviction (not a proof) that an envelope exists, and how it looks like (if it exists), namely 2 components, singular points, etc. In order to have an analytic description (either implicit or parametric or both) for the envelope a CAS can be used. A first pathway for this study is to use the standard **solve** commands of the CAS. For the above example, the code reads as follows:

```
> restart; with(plots);
> f := (y-t^2)^2+(x-t)^2-(3/2)^2;
> derf := diff(f, t);
> solve(‘and‘(f = 0, derf = 0), [x, y]);
```

The result reads as follows, enhancing the conviction that the envelope has two components

$$\left[x=-\frac{t(2t^2\sqrt{4t^2+1}+3)}{\sqrt{4t^2+1}}+2t^3+t, y=\frac{1}{2}\cdot\frac{2t^2\sqrt{4t^2+1}+3}{\sqrt{4t^2+1}}\right]$$
$$\left[x=-\frac{t(2t^2\sqrt{4t^2+1}+3)}{\sqrt{4t^2+1}}+2t^3+t, y=\frac{1}{2}\cdot\frac{2t^2\sqrt{4t^2+1}+3}{\sqrt{4t^2+1}}\right]$$

Of course, if 1.5 is entered instead of 3/2, the result looks "less elegant". Anyway, a plot of the curve may not be obtained in one shot, but has to be plotted as the union of separate plots. Still less elegant is the result, when a trigonometric parametrization is used for the circles.

Because of the square roots, this parametrization requires some work in order to try and transform it into a rational one, and then into a polynomial one. Anyway, with CAS assisted computations it is possible to differentiate the functions $x(t), y(t)$ and then look for singular points, whence determining the cusps which appeared in the experimental plot. Using a polynomial presentation, which is not always possible, then using an elimination order, could be less efficient for discovering singularities.

If the defining equations of the problem are polynomial, the problem can be automated and treated using Gröbner bases algorithms: an implicit equation is obtained. The same visualization problem as described in Section 2 appears: the plot obtained with an **implicitplot** or **implicitplot3d** command may be non accurate, because of the choice of the mesh and the required interpolations, as shown in figure 4. This issue has been studied in [8].

As far as visualization is concerned, transition to parameterized families of surfaces in 3-dimensional space is critical (for a precise definition and how to manage that, see [7]). In the new setting, the dynamical features we used previously are not available anymore: no slider bar is available, and moving a point as we did

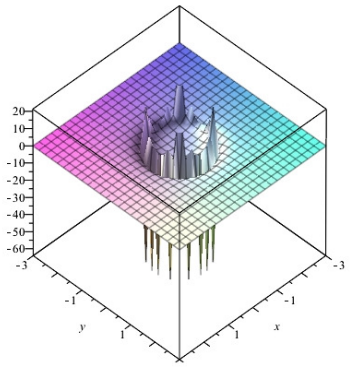


Figure 4: Non accurate plot

in 2D seems irrelevant. The experimental work based on Dynamical Geometry is impossible (we wish that further developments in CAS and DGS will provide this feature in the next future). Here the standard procedures of a CAS have to be used. In particular, if the data is polynomial, Gröbner bases algorithms can be used. We recalled already that rational data can be transformed into a polynomial setting.

The transition to parameterized families of curves and surfaces in 3D space rely on the same techniques. For a 1-parameter family of surfaces, the defining equations for an envelope are now:

$$\begin{cases} f(x,y,z,t) & = 0 \\ \frac{\partial f}{\partial t} f(x,y,z,t) & = 0 \end{cases} \tag{4}$$

New issues have to be dealt with: the general visualization problems, the availability of appropriate features in the software, etc. For the family of planes given by the equation $x+ty+t^2z=t^3$, where t is a real parameter, an envelope can be found, shown in Figure 5. A cuspidal edge appears, as for every 1-parameter family of planes. In order to understand the surface visually, dynamical features of the software are a must. Otherwise, at least two stills pictures have to been plotted. Actually the plot may be revolved with the mouse. In particular, the structure of the envelope as a ruled surface can be revealed visually using technology. In [8], we mentioned the influence of the choice of the mesh for plotting surfaces in 3D space on understanding the situation. For example, in Figure 5, tangents to the cuspidal edge generate the plot; this is a central feature of such an envelope.

The same work may be performed for 2-parameter families of surfaces. For example, consider the family of planes given by the equation $x+(a+b)y+(a^2+b^2)z=a^3+b^3$, where ua,b are real parameters. Here are a few rows of Maple code for an automated study of this envelope:

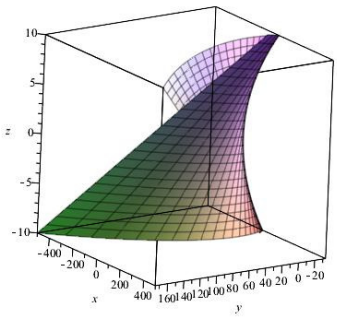


Figure 5: Exploration of the envelope of a family of planes

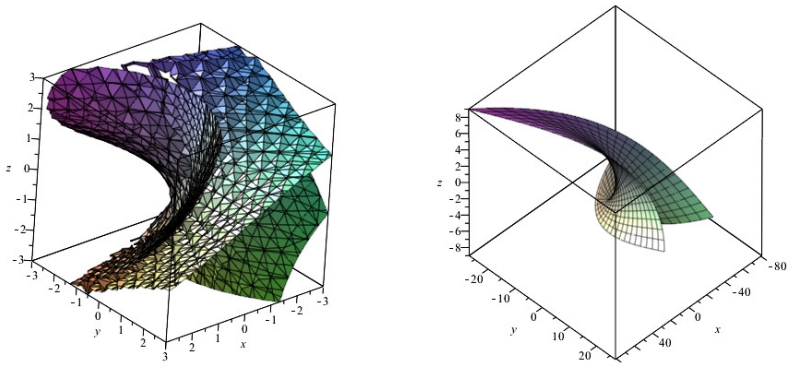
```
> restart; with(plots); with(PolynomialIdeals);
> f := x+(a+b)*y+(a^2+b^2)*z-a^3-b^3;
> daf := diff(f, a); dbf := diff(f, b);
> K := `<,>`(f, daf, dbf);
> KE := EliminationIdeal(K, {x, y, z});
> IdealInfo[Generators](KE);
> F:=%[1];
```

The result is the following polynomial:

$$F(x,y,z) = -729x^3 - 1458x^2yz + 432y^3x - 324z^3x^2 - 540z^2y^2x \\ + 288y^4z - 288z^4xy + 136z^3y^3 - 32z^6x + 16y^2z^5.$$

Implicit plot of this polynomial provides the displays in Figure 6.

A qualitative analysis reveals the existence of a cuspidal edge, and that the generators of the surface appear as curves tangent to the cuspidal edge. Actually the 1-parameter family described previously is a subfamily of the present 2-parameter family (e.g. for $b = 0$). Such a study provides an opportunity to discover new topics beyond the scope of the regular undergraduate curriculum, sometimes together with applications to practical situations. New computation skills with technology may be developed, in particular for the experimental aspect of the work (e.g., exploring the existence of cusps, as in Figure 1b). For this, the availability in the software of a slider bar is a central issue. Moreover, ability to switch between different registers of representation may be improved, within mathematics themselves (parametric vs implicit) and with the computer (algebraic, graphical, etc.). Anyway, we must be aware that the transition form 2D to 3D is a critical one, as



(a) Implicit Plot (b) Parametric Plot

Figure 6: Exploration of the envelope of a 2-parameter family of planes

the technology does not provide as many dynamical tools in 3D as in 2D, and the visualization skills of students are generally much better in 2D than in 3D .

The algebraic engine we used in different CAS was the commands based on computations of Gröbner bases in order 1) to solve the given system of equations, which yields a parametric representation of the envelopes, and 2) to look for an implicitization of this parametric representation. When such an implicitization is not to be found, algorithms exist for an approximate implicitization (see [4] and [5]).

References

[1] Dana-Picard, Th. *Motivating constraints of a pedagogy embedded Computer Algebra System*, International Journal of Science and Mathematics Education 5 (2), 217-235 (2007)

[2] Dana-Picard, Th., Mann, G. and Zehavi, N. *Bisoptic curves of a hyperbola*, International Journal of Mathematical Education in Science and Technology **45 (5)**, pp. 762-781 (2014).

[3] Dana-Picard, Th. and Zehavi, N. *Revival of a Classical Topic in Differential Geometry: Envelopes of Parameterized Families of Curves and Surfaces*, ACA 2015, Kalamata, Greece (2015).

[4] Pottman, H. and Peternell, M.: *Envelopes - Computational Theory and Applications.* In: Proceedings of Spring Conference in Computer Graphic, Budmerice, Slovakia, 3-23 (2000).

[5] Schultz T. and Juttler B. *Envelope computation in the plane by approximate implicitization,* Applicable Algebra in Engineering, Communication and Computing **22** (4), 265-288 (2011). doi: 10/1007/s00200-011-0149-1

[6] Trouche, L.. *Environnements informatisés et Mathématiques: Quels usages pour quels apprentissages?*, Educational Studies in Mathematics, 55(2004), 181-197 (2004)

[7] Yerushalmy, M. Challenging Known Transitions: Learning and Teaching Algebra with Technology, For the Learning of Mathematics 25(3),37-42 (2005).

[8] Zeitoun D. and Dana-Picard Th. *Accurate visualization of graphs of functions of two real variables*, International Journal of Computational and Mathematical Sciences 4(1), 1-11 (2010). Available: http://www.waset.org/journals/ijcms/v4/v4-1-1.pdf

About Giac's Gröbner basis and ideal elimination computation

B. Parisse[1]

[1] *University of Grenoble, France, bernard.parisse@ujf-grenoble.fr*

Automatic theorem proving is obviously an interesting feature in geometry softwares (cf. [3] and references therein), conversely classical geometry theorems may be used to check correctness and speed of the computing kernel of a CAS. In this talk, we will focus on Giac Groebner basis algorithm (based on [2] and [1]) and elimination algorithm, which plays a preponderant role in geometry automatic theorem proving and we will discuss correctness vs. speed (probabilistic vs. deterministic algorithm choice).

References

[1] E. A. Arnold. Modular algorithms for computing Gröbner bases . *Journal of Symbolic Computation*, 35(4):403–419, 2003.

[2] J.-C. Faugère. A new efficient algorithm for computing Gröbner bases (F4). *Journal of Pure and Applied Algebra*, 139(1–3):61–88, June 1999.

[3] Z. Kovács. *Computer Based Conjectures and Proofs in Teaching Euclidean Geometry*. PhD thesis, PhD thesis, JKU Linz, 2015.

What does ‘without loss of generality’ mean?

J. Davenport[1]

[1] *University of Bath, United Kingdom*

When one goes from a geometrical statement to an algebraic statement, the immediate translation is to replace every point by a pair of coordinates. A statement with N points is then a statement with $2N$ variables, and the complexity of tools like cylindrical algebraic decomposition is doubly exponential in the number of variables. Hence one says ‘without loss of generality, A is at $(0,0)$’ and so on. How might one automate this, or turn it into a procedure (and possibly even a formal proof).

Towards higher-degree quantifier elimination by virtual substitution

T. Sturm[1]

[1] *CNRS Research Director, LORIA Nancy, France*
Senior Researcher, MPI Informatik, Germany
http://www.loria.fr/~tsturm/

We give an overview of methods and implementations of real quantifier elimination (QE) and variants and their application to various geometric problems including automated proving, computational geometry, and constructive solid geometry. Variants include generic QE, which produces non-degeneracy conditions, and extended QE, which produces sample point with satisfiable existential problems. We furthermore highlight recent research on theoretical foundations and implementation techniques for virtual substitution-based QE, which have to potential to lead to significant progresses with geometric applications in the near future. All discussed methods are available with the free and open-source system Reduce/Redlog under a very liberal Free-BSD license.

S10
Computer Algebra in Coding Theory and Cryptography

On multivariable asymmetric public-key cryptography based on simultaneous algebraic Riccati equations over finite fields

Y. Peretz[1]

[1] *Computer Sciences Department, Lev Academic Center, Jerusalem, Israel. yosip@g.jct.ac.il*

Many encryption schemes based on Multivariable Quadratic Equations (MQE) over finite fields were suggested in the last three decades and many were broken (see [1]). Apparently, the broken systems were based on some hidden structure, which on one hand enabled the efficient invertibility of the system, but on the other hand was found to be vulnerable to algebraic attacks. Almost all the MQE based encryption schemes that were proved to be insecure, share the common drawback that some quadratic forms associated to their central maps have low rank (see [2]) and therefore are vulnerable to the Min-Rank Attack (see [3]). On the other hand, the belief that random quadratic systems are hard to solve on average (see [4], [5] and references therein), points towards designing trap-door primitives based on randomness, which raises difficulties in designing immune invertible primitives. Little was done in this direction in the context of asymmetric public-key cryptography (see [4]).

An overview of Multivariate Public-Key Cryptography (MPKC) is given in [6], where the authors call for a unifying framework for cryptanalysis of MPKC systems in order to build confidence in their security. They also point out to potential applications of such systems in the realm of limited computing power (e.g. in Radio Frequency Identification Devices (RFID) and in Wireless Sensing (WS)), where other cryptographic systems (e.g. RSA, ELGAMAL, ECC) are irrelevant. A summary of the main developments in the cryptanalysis of multivariate cryptosystems is given in [7] and [5].

Let $\mathbf{F}$ denote any finite field. Non-symmetric Algebraic Riccati Equation (ARE) over $\mathbf{F}$ is an equation of the form:

$$XCX + XD - AX - B = 0, \tag{1}$$

where A, B, C, D are $m \times m, m \times n, n \times m, n \times n$ matrices and the solution X is a $m \times n$ matrix over $\mathbf{F}$. The complexity of computing X is equivalent to the complexity of the constrained generalized eigenvalue-eigenvector problem defined by:

$$T \begin{bmatrix} X \\ I \end{bmatrix} = \begin{bmatrix} X \\ I \end{bmatrix} L, \tag{2}$$

where

$$T = \begin{bmatrix} A & B \\ C & D \end{bmatrix}, \tag{3}$$

and $L = CX + D$ is $n \times n$ matrix. The Non-symmetric Simultaneous Algebraic Riccati Equations problem (NSARE) is the following: given t quadruples

$$(A_i, B_i, C_i, D_i), i = 1, \ldots, t, \tag{4}$$

find X such that all the equations:

$$XC_iX + XD_i - A_iX - B_i = 0, \tag{5}$$

are satisfied simultaneously for $i = 1, \ldots, t$. The NSARE is known to be NP-complete over any finite field and NP-hard over any infinite field (see [8]).
It follows that any set of multivariable polynomial equations can be reduced (by polynomial-time reduction) to the NSARE problem (the converse is obvious) and thus any encryption scheme based on multivariable polynomial set of equations can be crypt-analyzed to vulnerabilities by investigating the related equivalent NSARE problem.

Based on the NSARE problem, pubic-key encryption schemes were defined, with the following features (see [8]):

1. The security of the systems is based on provable NP-complete problem.

2. The suggested schemes fit to the age of post-quantum cryptography.

3. The systems involves truly (pseudo) random choice of the coefficients of the core equations.

4. The suggested scheme is very flexible in the ability of matching the security level to the needs and to the given computing power.

5. The suggested systems fit to the realm of limited-power computing devices since they involve only matrix summation and multiplication (matrix inversion is made once for the whole system life).

6. The suggested systems has a very fast encryption and decryption time. It has several magnitudes of improvement over the RSA for equivalent level of security.

7. The suggested schemes are highly parallelizable in parallel software or hardware and thus the encryption and decryption time can be speeded-up to a fantastic time.

Finally, the urgent call for new multivariable public-key cryptosystems (see [9]) and the call for a unifying framework for cryptanalysis of MPKC systems (see [6]) are also fulfilled by this research.

References

[1] C. Wolf, B. Preneel, *Taxonomy of Public-Key Schemes based on the Problem of Multivariate Quadratic Equations*, Cryptology ePrint Archive, Report 2005/077, http://eprint.iacr.org/ (2005).

[2] C. Tao, A. Diene, S. Tang and J. Ding, *Simple Matrix Scheme for Encryption*, PQCrypto 2013, LNCS 7932, pp. 231-242 (2013).

[3] A. Kipnis, A. Shamir, *Cryptanalysis of the HFE public key cryptosystem by relinearization*, CRYPTO 1999, LNCS 1666, pp. 19-30 (1999).

[4] N. T. Courtois, *General Principles of Algebraic Attacks and New Design Criteria for Cipher Components*, Advanced Encryption Standard - AES 2005, LNCS 3373, pp. 67-83 (2005).

[5] O. Billet, J. Ding, *Overview of Cryptanalysis Techniques in Multivariate Public Key Cryptography*, Inbook: Gröbner Bases, Coding, and Cryptography, Editors: M. Sala, T. Mora, L. Perret, S. Sakata and C. Traverso, Springer-Verlag Berlin Heidelberg, pp.263-283 (2009).

[6] J. Ding, B. Y. Yang, *Multivariate Public Key Cryptography*, Inbook: Post Quantum Cryptography, Editors: D. J. Bernstein, J. Buchmann and E. Dahmen, Springer-Verlag Berlin Heidelberg, pp.193-234 (2009).

[7] Jintai Ding, Jason E. Gower, Dieter S. Schmidt, *Multivariate Public Key Cryptosystems*, Series: Advances in Information Security, Editor: Sushil Jajodia, Springer (2006).

[8] Y. Peretz, *On mulivariable encryption schemes based on simultaneous algebraic Riccati equations over finite fields*, Finite Fields and Their Applications, 39, pp. 1-35 (2016).

[9] W. Shen, S. Tang, *TOT, a Fast Multivariable Public Key Cryptosystem with Basic Secure Trapdoor*, Cryptology ePrint Archive, Report 2013/771, http://eprint.iacr.org/ (2013).

Is it hard to retrieve an error-correcting pair?

Irene Márquez-Corbella and Ruud Pellikaan

Dept. of Mathematics, Statistics and O. Research, University of La Laguna, Spain.
irene.marquez.corbella@ull.es
Dept. of Mathematics and Computing Science, Eindhoven University of Technology, P.O. Box 513, 5600 MB Eindhoven, The Netherlands. g.r.pellikaan@tue.nl

Code-based cryptography is an interesting alternative to classic number-theory Public-Key Cryptosystems (PKC) since it is conjectured to be secure against quantum computer attacks. Many families of codes have been proposed for these cryptosystems. One of the main requirements is having high performance t-bounded decoding algorithms which is achieved in the case the code has a t-error-correcting pair (ECP). The class of codes with a t-ECP is proposed for the McEliece cryptosystem. The hardness of retrieving the t-ECP for a given code is considered. To this end we have to solve a large system of bilinear equations. Two possible induction procedures are considered, one for sub/super ECP's and one by puncturing/shortening. In both procedures in every step only a few bilinear equations need to be solved.

1 Notation and Prerrequisites

By $\mathbb{F}_q$, where q is a prime power, we denote a finite field with q elements. An $[n,k]$ linear code $\mathscr{C}$ over $\mathbb{F}_q$ is a k-dimensional subspace of $\mathbb{F}_q^n$. We will denote the length of $\mathscr{C}$ by $n(\mathscr{C})$, its dimension by $k(\mathscr{C})$ and its minimum distance, $d(\mathscr{C})$.

Given two elements $\mathbf{a}$ and $\mathbf{b}$ on $\mathbb{F}_q^n$, the *star multiplication* is defined by coordinatewise multiplication, that is, $\mathbf{a}*\mathbf{b} = (a_1b_1,\ldots,a_nb_n)$. Then, $A*B$ is the code in $\mathbb{F}_q^n$ generated by $\{\mathbf{a}*\mathbf{b} \mid \mathbf{a}\in A \text{ and } \mathbf{b}\in B\}$.

The *standard inner multiplication* of $\mathbf{a}$ and $\mathbf{b}$ on $\mathbb{F}_q^n$ is defined by $\mathbf{a}\cdot\mathbf{b} = \sum_{i=1}^n a_ib_i$. Now $A\perp B$ if and only if $\mathbf{a}\cdot\mathbf{b}=0$ for all $\mathbf{a}\in A$ and $\mathbf{b}\in B$.

Definition 1 *Let C be an $\mathbb{F}_q$-linear code of length n. The pair (A,B) of $\mathbb{F}_{q^m}$-linear codes of length n is called a t-error correcting pair (ECP) for C if the following properties holds:*

E.1 $(A*B)\perp C$,

E.2 $k(A) > t$,

E.3 $d(B^\perp) > t$,

E.4 $d(A)+d(C) > n$.

Broadly speaking: given a positive integer t, a t-ECP for a linear code $C\subseteq F_q^n$ is a pair of linear codes (A,B) satisfying that $A*B\subseteq C^\perp$ together with several

inequalities relating t and the dimensions and (dual) minimum distances of A, B and C. Furthermore note that if the fourth property (E.4) is replaced by the statements presented below then, again (A,B) is a t-ECP for C and the minimum distance of such linear code is at least $2t+1$.

E.5 $d(A^{\perp}) > 1$ or equivalently A is a non-degenerated code,

E.5 $d(A) + 2t > n$.

Error-correcting pairs (ECP) were introduced and studied in [4, 7, 8], as a general algebraic method of decoding linear codes. It was shown that an $[n, n-2t, 2t+2]$ code has a t-error correcting pair if and only if it is a Generalized Reed-Solomon code [6]. The concept of an ECP is instrumental in the polynomial attack of the McEliece cryptosystem that uses algebraic geometry codes [2].

2 The McEliece PKC system using ECP's

The class of codes with a t-ECP is proposed for the McEliece cryptosystem [5]. The hardness of retrieving the t-ECP for a given code is considered. To this end we have to solve a large system of bilinear equations [3, 1]. Two possible induction procedures are considered, one for sub/super ECP's and one by puncturing/shortening. In both procedures in every step only a few bilinear equations need to be solved.

Let $\mathscr{P}(n,t,q)$ be the collection of pairs (A,B) such that there exist a positive integer m and a pair (A,B) of $\mathbb{F}_{q^m}$-linear codes of length n that satisfy the conditions E.2, E.3, E.5 and E.6.

Let C be the $\mathbb{F}_q$-linear code of length n that is the subfield subcode that has the elements of $A*B$ as parity checks

$$C = \mathbb{F}_q^n \cap (A*B)^{\perp}$$

Then the minimum distance of C is at least $2t+1$ and (A,B) is a t-ECP for C

Let $\mathscr{F}(n,t,q)$ be the collection of $\mathbb{F}_q$-linear codes of length n and minimum distance $d \geq 2t+1$.

Consider the following map

$$\begin{array}{rccc} \varphi_{(n,t,q)}: & \mathscr{P}(n,t,q) & \longrightarrow & \mathscr{F}(n,t,q) \\ & (A,B) & \longmapsto & C \end{array}$$

The question is whether this map is a one-way function.

We treat the entries of the generator matrices of the the pair of codes (A,B) as variables X_{ij} and Y_{ij}. The condition $(A*B) \perp C$ becomes a system of bilinear

equations. We will apply the F_5-method to find Gröbner basis for a solution [3, 1]. The puncturing and shortening procedure that was used in [6] will reduce the number of variables.

References

[1] M. Bardet, J.-C. Faugère, B. Salvy, and P.-J. Spaenlehauer. On the complexity of solving quadratic boolean systems. *CoRR*, abs/1112.6263, 2011.

[2] A. Couvreur, I. Márquez-Corbella, and R. Pellikaan. Cryptanalysis of public-key cryptosystems that use subcodes of algebraic geometry codes. *ArXiv e-prints 1409.8220*, September 2014.

[3] J.-C. Faugère, M. Safey El Din, and P.-J. Spaenlehauer. Gröbner bases of bihomogeneous ideals generated by polynomials of bidegree $(1,1)$: algorithms and complexity. *J. Symbolic Comput.*, 46(4):406–437, 2011.

[4] R. Kötter. A unified description of an error locating procedure for linear codes. In *Proceedings of Algebraic and Combinatorial Coding Theory*, pages 113–117. Voneshta Voda, 1992.

[5] I. Márquez-Corbella and R. Pellikaan. Error-correcting pairs for a public-key cryptosystem. *ArXiv e-prints 1205.3647v1*, 2012.

[6] Irene Márquez-Corbella and Ruud Pellikaan. A characterization of mds codes that have an error correcting pair. *Finite Fields Appl.*, 40(C):224–245, July 2016.

[7] R. Pellikaan. On decoding by error location and dependent sets of error positions. *Discrete Math.*, 106–107:369–381, 1992.

[8] R. Pellikaan. On the existence of error-correcting pairs. *Statistical Planning and Inference*, 51:229–242, 1996.

Solving the Binary Puzzle

P. Utomo[1], R. Makarim[2]

[1] *Eindhoven University of Technology, Netherlands, p.h.utomo@tue.nl*
[2] *Mathematical Institute, University Leiden and Centrum Wiskunde en Informatica, Netherlands makarim@cwi.nl*

Binary puzzle is a sudoku-like puzzle with values in each cell taken from the set $\{0,1\}$. We look at the mathematical theory behind it. A solved binary puzzle is an $n \times n$ (n even) binary array that satisfies the following conditions:

1. No three consecutive ones and also no three consecutive zeros in each row and each column,
2. Every row and column is balanced, that is the number of ones and zeros must be equal in each row and in each column,
3. Every two rows and every two columns must be distinct.

Figure 1 is an example of initial setting of a binary puzzle. There is only one solution satisfying all three conditions which can be seen in Figure 2. Binary puzzles can be seen as constrained arrays [3]. One can also see this array from an erasure correcting point of view [2].

This paper focuses on solving binary puzzles. Solving binary puzzle is proven to be an NP-complete problem[1]. We devise and compare three approaches for finding its solution. The first solves straightforwardly by means of exhaustive search. The second idea, transforms the problem into a SAT problem, then we solve using a SAT solver. The third approach construct a set of polynomial equations over $\mathbb{F}_2$ representing the three conditions for a solved binary puzzle. The variables in the system of equations correspond to all cells in the puzzle. Hence

	0						
			1		1		0
		0					
	1						
				1			
	0				1		
	0			0			
				0		0	

Figure 1: Unsolved Puzzle

1	0	1	0	1	0	1	0
0	1	0	1	0	1	1	0
1	0	0	1	1	0	0	1
0	1	1	0	0	1	1	0
0	1	0	1	1	0	0	1
1	0	1	0	1	1	0	0
1	0	0	1	0	0	1	1
0	1	1	0	0	1	0	1

Figure 2: Solved Puzzle

the solution for the equation system is a solution for the puzzle and it can be obtained by computing its Gröbner basis.

From a complexity point of view, solving the puzzle straightforwardly is more efficient in terms of execution time. The comparison between the three methods in solving the puzzle of various sizes is given in the Table 1. All the computation is done in SageMath 7.0.

Table 1: Comparison of execution time (in seconds) for each method.

Size	SAT		Goebner basis		Exhaustive search
	Pre-comp.	Solver	Pre-comp.	Solver	
4×4	0.01	0.05	0.02	0.05	0.01
6×6	0.14	0.26	0.11	0.06	0.16
8×8	1.58	2.20	0.53	0.13	0.12
10×10	12.31	16.45	3.30	8.69	0.48
12×12	85.43	107.80	47.80	4.55	3.89
14×14	-	-	-	-	94.32

References

[1] M. De Biasi, Binary puzzle is NP-complete, `http://nearly42.org`

[2] P. Utomo and R. Pellikaan, Binary Puzzles as an Erasure Decoding Problem. *Proc. 36th WIC Symp. on Information Theory in the Benelux*, pp. 129–134 May 2015. `http://www.w-i-c.org/proceedings/proceedings_SITB2015.pdf`.

[3] P. Utomo and R. Pellikaan, On The Rate of Constrained Arrays. *Proc. IndoMS International Conference on Mathematics and Its Applications (IICMA) 2015*, 3 November 2015. `http://www.win.tue.nl/~ruudp/paper/75.pdf`

Generalized Hadamard Additive Codes

S. T. Dougherty[1], J. Rifà[2], M. Villanueva[2]

[1] *University of Scranton, Scranton, USA, steven.dougherty@scranton.edu*
[2] *Universitat Autònoma de Barcelona, Spain, {josep.rifa, merce.villanueva}@uab.cat*

This work was partially supported by the Spanish MINECO under Grants TIN2013-40524-P and MTM2015-69138-REDT, and by the Catalan AGAUR under Grant 2014SGR-691.

Let $\mathbb{F}_q = \mathrm{GF}(q)$ denote the finite field with q elements, where $q = p^e$, p prime. Let $\mathbb{F}_q^n$ be the vector space of dimension n over $\mathbb{F}_q$. The *Hamming distance* between vectors $\mathbf{w}$, $\mathbf{v} \in \mathbb{F}_q^n$, denoted by $d(\mathbf{w},\mathbf{v})$, is the number of coordinates in which $\mathbf{w}$ and $\mathbf{v}$ differ. A *code* C over $\mathbb{F}_q$ of length n is a nonempty subset of $\mathbb{F}_q^n$. The elements of C are called *codewords*. The *minimum distance* of a code is the smallest Hamming distance between any pair of distinct codewords. A code C over $\mathbb{F}_q$ is called *linear* if it is a linear space over $\mathbb{F}_q$ and, it is called *K-additive* if it is a linear space over a subfield $K \subset \mathbb{F}_q$. The dimension of a K-additive code C over $\mathbb{F}_q$ is defined as the number k such that $q^k = |C|$. Note that k is not necessarily an integer, but ke is an integer, where $q = |K|^e$. Two codes C_1, $C_2 \subset \mathbb{F}_q^n$ are said to be *permutation equivalent* if there exists a permutation σ of the n coordinates such that $C_2 = \{\sigma(c_1,c_2,\ldots,c_n) = (c_{\sigma^{-1}(1)},\ldots,c_{\sigma^{-1}(n)}) : (c_1,c_2,\ldots,c_n) \in C_1\}$, [2], [6]. Without loss of generality, we shall assume, unless stated otherwise, that the all-zero vector, denoted by $\mathbf{0}$, is in C.

Two structural parameters of (nonlinear) codes are the dimension of the linear span and the kernel. The *linear span* of a code C over $\mathbb{F}_q$, denoted by $\mathscr{R}(C)$, is the subspace over $\mathbb{F}_q$ spanned by C, that is $\mathscr{R}(C) = \langle C \rangle$. The dimension of $\mathscr{R}(C)$ is called the *rank* of C and is denoted by $\mathrm{rank}(C)$. If $q = p^e$, p prime, we can also define $\mathscr{R}_p(C)$ and $\mathrm{rank}_p(C)$ as the subspace over $\mathbb{F}_p$ spanned by C and its dimension, respectively. The *kernel* of a code C over $\mathbb{F}_q$, denoted by $\mathscr{K}(C)$, is defined as $\mathscr{K}(C) = \{\mathbf{x} \in \mathbb{F}_q^n \ : \ \alpha\mathbf{x} + C = C \text{ for all } \alpha \in \mathbb{F}_q\}$. If $q = p^e$, p prime, we can also define the *p-kernel* of C as $\mathscr{K}_p(C) = \{\mathbf{x} \in \mathbb{F}_q^n \ : \ \mathbf{x} + C = C\}$. Since we assume that $\mathbf{0} \in C$, then $\mathscr{K}(C)$ is a linear subcode of C and $\mathscr{K}_p(C)$ is an $\mathbb{F}_p$-additive subcode. We denote the dimension of the kernel (resp., p-kernel) of C by $\ker(C)$ (resp., $\ker_p(C)$). These concepts were first defined in [9] for codes over $\mathbb{F}_q$, generalizing the binary case described previously in [1], [8]. In [9], it was proved that the code C over $\mathbb{F}_q$ can be written as the union of cosets of $\mathscr{K}(C)$ (resp., $\mathscr{K}_p(C)$), and $\mathscr{K}(C)$ (resp., $\mathscr{K}_p(C)$) is the largest such linear code over $\mathbb{F}_q$ (resp., $\mathbb{F}_p$) for which this is true. Moreover, it is clear that $\mathscr{K}(C) \subseteq \mathscr{K}_p(C)$.

A *generalized Hadamard* (GH) *matrix* $H(q,\lambda) = (h_{ij})$ of order $n = q\lambda$ over $\mathbb{F}_q$ is a $q\lambda \times q\lambda$ matrix with entries from $\mathbb{F}_q$ with the property that for every i, j,

$1 \le i < j \le q\lambda$, each of the multisets $\{h_{is} - h_{js} : 1 \le s \le q\lambda\}$ contains every element of $\mathbb{F}_q$ exactly λ times. It is known that since $(\mathbb{F}_q, +)$ is an abelian group then $H(q,\lambda)^T$ is also a GH matrix, where $H(q,\lambda)^T$ denotes the transpose of $H(q,\lambda)$ [5]. An ordinary Hadamard matrix of order 4μ corresponds to a GH matrix $H(2,\lambda)$ over $\mathbb{F}_2$, where $\lambda = 2\mu$.

Two GH matrices H_1 and H_2 of order n are said to be *equivalent* if one can be obtained from the other by a permutation of the rows and columns and adding the same element of $\mathbb{F}_q$ to all the coordinates in a row or in a column. We can always change the first row and column of a GH matrix into zeros and we obtain an equivalent GH matrix which is called *normalized*. From a normalized Hadamard matrix H, we denote by F_H the code over $\mathbb{F}_q$ consisting of the rows of H, and C_H the one defined as $C_H = \bigcup_{\alpha \in \mathbb{F}_q} (F_H + \alpha \mathbf{1})$, where $F_H + \alpha \mathbf{1} = \{\mathbf{h} + \alpha \mathbf{1} : \mathbf{h} \in F_H\}$ and $\mathbf{1}$ denotes the all-one vector. The code C_H over $\mathbb{F}_q$ is called *generalized Hadamard* (GH) *code*. Note that F_H and C_H are generally nonlinear codes over $\mathbb{F}_q$.

To check whether two GH matrices are equivalent is known to be an NP-hard problem. However, we can use the invariants related to the linear span and kernel of the corresponding GH codes in order to help in their classification, since if two GH codes have different ranks or dimensions of the kernel, the GH matrices are nonequivalent.

The rank and dimension of the kernel for ordinary Hadamard codes over $\mathbb{F}_2$ have been studied. Specifically, lower and upper bounds for these two parameters were established, and the construction of an Hadamard code for all allowable ranks and dimensions of the kernel between these bounds was given [10], [11]. Moreover, the rank and dimension of the kernel for each nonisomorphic $\mathbb{Z}_2\mathbb{Z}_4$-linear Hadamard code were also established [12]. The $\mathbb{Z}_2\mathbb{Z}_4$-linear codes are the Gray map image of $\mathbb{Z}_2\mathbb{Z}_4$-additive codes, which are subgroups of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$. Some of these results have been generalized to GH codes over $\mathbb{F}_q$ [3]. In this paper, we continue studying the rank and dimension of the kernel for GH codes over $\mathbb{F}_q$. Now, we focus on an specific family of GH codes, namely the GH additive codes, that is, additive codes obtained from GH matrices.

1 Kronecker sum construction

A standard method to construct GH matrices from other GH matrices is given by the *Kronecker sum construction* [7], [13]. That is, if $H(q,\lambda) = (h_{ij})$ is any $q\lambda \times q\lambda$ GH matrix over $\mathbb{F}_q$, and $B_1, B_2, \ldots, B_{q\lambda}$ are any $q\mu \times q\mu$ GH matrices over $\mathbb{F}_q$, then the matrix in Table 1 gives a $q^2\lambda\mu \times q^2\lambda\mu$ GH matrix over $\mathbb{F}_q$, denoted by $H \oplus [B_1, B_2, \ldots, B_n]$, where $n = q\lambda$. If $B_1 = B_2 = \cdots = B_n = B$, then we write $H \oplus [B_1, B_2, \ldots, B_n] = H \oplus B$.

$$H \oplus [B_1, B_2, \ldots, B_n] = \begin{pmatrix} h_{11}+B_1 & h_{12}+B_1 & \cdots & h_{1n}+B_1 \\ h_{21}+B_2 & h_{22}+B_2 & \cdots & h_{2n}+B_2 \\ \vdots & \vdots & \vdots & \vdots \\ h_{n1}+B_n & h_{n2}+B_n & \cdots & h_{nn}+B_n \end{pmatrix}$$

Table 1: Kronecker sum construction

Let S_q be the normalized GH matrix $H(q,1)$ given by the multiplicative table of $\mathbb{F}_q$. As for ordinary Hadamard matrices over $\mathbb{F}_2$, starting from a GH matrix $S^1 = S_q$, we can recursively define S^t as a GH matrix $H(q, q^{t-1})$, constructed as $S^t = S_q \oplus [S^{t-1}, S^{t-1}, \ldots, S^{t-1}] = S_q \oplus S^{t-1}$ for $t > 1$, which is called a *Sylvester* GH *matrix*.

2 Generalized Hadamard $\mathbb{F}_p$-additive codes

In this section, we state some new results on generalized Hadamard additive codes.

Proposition 2.1 *Let $H(q,\lambda)$ be a* GH *matrix over $\mathbb{F}_q$, where $q = p^e$, p prime, and $e > 1$. Let $n = q\lambda = p^t s$ such that* $\gcd(p,s) = 1$. *Then*

(i) If C_H is an $\mathbb{F}_p$-additive code, then $s = 1$.

(ii) The code C_H is an $\mathbb{F}_p$-additive code if and only if

$$\mathrm{rank}_p(C_H) = \ker_p(C_H) = 1 + t/e.$$

(iii) If C_H is an $\mathbb{F}_p$-additive code and $\ker(C_H) = k$, *then*

$$\frac{e+t-k}{e-1} \leq \mathrm{rank}(C_H) \leq 1 + t - (e-1)(k-1).$$

(iv) If C_H is an $\mathbb{F}_p$-additive code and $\ker(C_H) = k$, *then $k = 1 + t/e$ when C_H is linear over $\mathbb{F}_q$ (t is a multiple of e), or $1 \leq k \leq \lfloor t/e \rfloor$ otherwise.*

We introduce a new construction of GH codes which allows us to guarantee that the obtained code C_H of length $n = p^t$ is $\mathbb{F}_p$-additive, has kernel of minimum dimension 1, and maximum rank $t+1$.

Proposition 2.2 *For $q = p^e$, p prime, and any $t > e > 1$, there exists a* GH *matrix $H(p^e, p^{t-e})$ such that C_H is an $\mathbb{F}_p$-additive code over $\mathbb{F}_{p^e}$ of length $n = p^t$ with* $\ker(C_H) = 1$ *and* $\mathrm{rank}(C_H) = t+1$.

Example 2.3 *In this example, we construct a* GH *matrix* $H(2^2,2)$ *such that* C_H *is an* $\mathbb{F}_2$*-additive code over* $\mathbb{F}_{2^2}$ *of length* $n = 2^3$ *with* $\ker(C_H) = 1$ *and* $\operatorname{rank}(C_H) = 4$. *We begin with the* GH *matrix* $H(2^3,1)$ *given by the multiplicative table of* $\mathbb{F}_{2^3}$, *where* ω *is a primitive element in* $\mathbb{F}_{2^3}$ *and* $\omega^3 = \omega + 1$.

$$H(2^3,1) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 \\ 0 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & 1 \\ 0 & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & 1 & \omega \\ 0 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & 1 & \omega & \omega^2 \\ 0 & \omega^4 & \omega^5 & \omega^6 & 1 & \omega & \omega^2 & \omega^3 \\ 0 & \omega^5 & \omega^6 & 1 & \omega & \omega^2 & \omega^3 & \omega^4 \\ 0 & \omega^6 & 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 \end{pmatrix} \tag{1}$$

Next, we write each entry of the matrix (1) using coordinates over $\mathbb{F}_2$ *and projecting over* $\mathbb{F}_{2^2}$. *By Proposition 2.2, we obtain the* GH *matrix* $H(2^2,2)$, *where* α *is a primitive element in* $\mathbb{F}_{2^2}$ *and* $\alpha^2 = \alpha + 1$. *Note that* $\bar{0} = \overline{(0,0,0)} = (0,0) = 0$, $\bar{1} = \overline{(1,0,0)} = (1,0) = 1$, $\overline{\omega} = \overline{(0,1,0)} = (0,1) = \alpha$, $\overline{\omega}^2 = \overline{(0,0,1)} = (0,0) = 0$, $\overline{\omega}^3 = \overline{(1,1,0)} = (1,1) = \alpha^2$, $\overline{\omega}^4 = \overline{(0,1,1)} = (0,1) = \alpha$, $\overline{\omega}^5 = \overline{(1,1,1)} = (1,1) = \alpha^2$, $\overline{\omega}^6 = \overline{(1,0,1)} = (1,0) = 1$.

$$H(2^2,2) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & \alpha & 0 & \alpha^2 & \alpha & \alpha^2 & 1 \\ 0 & \alpha & 0 & \alpha^2 & \alpha & \alpha^2 & 1 & 1 \\ 0 & 0 & \alpha^2 & \alpha & \alpha^2 & 1 & 1 & \alpha \\ 0 & \alpha^2 & \alpha & \alpha^2 & 1 & 1 & \alpha & 0 \\ 0 & \alpha & \alpha^2 & 1 & 1 & \alpha & 0 & \alpha^2 \\ 0 & \alpha^2 & 1 & 1 & \alpha & 0 & \alpha^2 & \alpha \\ 0 & 1 & 1 & \alpha & 0 & \alpha^2 & \alpha & \alpha^2 \end{pmatrix} \tag{2}$$

Proposition 2.4 *For* $q = p^e$, p *prime, and any* $t \geq e > 1$, *there exists a* GH $\mathbb{F}_p$*-additive code* C_H *over* $\mathbb{F}_q$ *of length* $n = p^t$ *with* $\ker(C_H) = k$ *if and only if*

(i) $k = 2$ *when* $t = e$,

(ii) $k \in \{1, \ldots, \lfloor t/e \rfloor\}$ *when* $e \nmid t$,

(iii) $k \in \{1, \ldots, t/e + 1\}$, *otherwise.*

Corollary 2.5 *For* $q = p^2$, p *prime, and any* $t \geq 2$, *there exists a* GH $\mathbb{F}_p$*-additive code* C_H *over* $\mathbb{F}_q$ *of length* $n = p^t$ *with* $\ker(C_H) = k$ *and* $\operatorname{rank}(C_H) = t + 2 - k$ *if and only if* k *is any of the allowable parameters given by Proposition 2.4.*

Example 2.6 *For $q = 4$, we have the following results:*

- *If $n = 4$, there is only one* GH *matrix $H(4,1)$ over $\mathbb{F}_4$ having* $\mathrm{rank}(C_H) = \mathrm{rank}_2(C_H) = \ker(C_H) = \ker_2(C_H) = 2$. *Therefore, C_H is a linear code and an $\mathbb{F}_2$-additive code, which corresponds to the Sylvester* GH *matrix $S^1 = S_4$.*
- *If $n = 8$, there is only one* GH *matrix $H(4,2)$ over $\mathbb{F}_4$ having* $\mathrm{rank}(C_H) = 4$ *and* $\ker(C_H) = 1$. *Therefore, C_H is nonlinear over $\mathbb{F}_4$. However, it has* $\mathrm{rank}_2(C_H) = \ker_2(C_H) = 2.5$*, so it is an $\mathbb{F}_2$-additive code.*
- *If $n = 16$, it is known that there are 226 nonequivalent* GH *matrices $H(4,4)$ over $\mathbb{F}_4$ [4], which satisfy that* $(\mathrm{rank}(C_H), \ker(C_H)) \in \{(3,3),(4,2),(4,1),(5,2),(5,1),(6,1),(7,1),(8,1)\}$ *[3]. Moreover, if we focus on the $\mathbb{F}_2$-additive codes, we have that they must satisfy* $\mathrm{rank}_2(C_H) = \ker_2(C_H) = 3$. *In this case,* $(\mathrm{rank}(C_H), \ker(C_H)) \in \{(3,3),(4,2),(5,1)\}$. *The first one corresponds to the Sylvester* GH *matrix S^2, which is also linear over $\mathbb{F}_4$.*

References

[1] H. Bauer, B. Ganter, and F. Hergert, "Algebraic techniques for nonlinear codes," Combinatorica, vol. 3, pp. 21–33, 1983.

[2] G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein, *Covering Codes*, North-Holland, 1997.

[3] S. T. Dougherty, J. Rifà, and M. Villanueva, "Ranks and kernels of codes from generalized Hadamard matrices," IEEE Trans. Inform. Theory, vol. 62(2), pp. 687–694, 2016.

[4] M. Harada, C. Lam, and V. Tonchev, "Symmetric $(4,4)$-nets and generalized Hadamard matrices over groups or order 4," Des. Codes Cryptography, vol. 34, pp. 71–87, 2005.

[5] D. Jungnickel, "On difference matrices, resolvable designs and generalized Hadamard matrices," Math. Z., vol. 167, pp. 49–60, 1979.

[6] F. I. MacWilliams and N. J. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, New York, 1977.

[7] Jong-Seon No and H.Y. Song, "Generalized Sylvester-type Hadamard matrices," IEEE International Symposium on Information Theory, pp. 472, June 2000.

[8] K. T. Phelps, M. LeVan, "Kernels of nonlinear Hamming codes," Des. Codes Cryptography, vol. 6, pp. 247–257, 1995.

[9] K. T. Phelps, J. Rifà, and M. Villanueva, "Kernels and p-kernels of p^r-ary 1-perfect codes," Des. Codes Cryptography, vol. 37, pp. 243–261, 2005.

[10] K. T. Phelps, J. Rifà, and M. Villanueva, "Rank and kernel of binary Hadamard codes," IEEE Trans. Inform. Theory, vol. 51, no. 11, pp. 3931–3937, 2005.

[11] K. T. Phelps, J. Rifà, and M. Villanueva, "Hadamard codes of length $2^t s$ (s odd): Rank and kernel," Lecture Notes in Computer Science, vol. 3857, pp. 328–337, 2006.

[12] K. T. Phelps, J. Rifà, and M. Villanueva, "On the additive (Z4-linear and non-Z4- linear) Hadamard codes: rank and kernel," IEEE Trans. Inform. Theory, vol. 52(1), pp. 316–319, 2006.

[13] S. S. Shrikhande, "Generalized Hadamard matrices and orthogonal arrays of strength two," Canad. J. Math., vol. 16, pp. 736–740, 1964.

Galois Theory for Linear Codes

A. Fotue Tabue[1] and E. Martínez-Moro[2] and C. Mouaha[1]

[1] *Department of mathematics, Faculty of Sciences, University of Yaoundé 1, Cameroon,* alexfotue@gmail.com, cmouaha@yahoo.fr
[2] *Institute of Mathematics, University of Valladolid, Spain,* Edgar.Martinez@uva.es

Let $\mathtt{R}$ a be finite chain ring of nilpotency index s, $\mathtt{S}$ the *Galois extension* of $\mathtt{R}$ of rank m, and G the group of ring automorphisms of $\mathtt{S}$ fixing $\mathtt{R}$. We will denote by $\mathscr{L}(\mathtt{S}^\ell)$ (resp. $\mathscr{L}(\mathtt{R}^\ell)$) the set of $\mathtt{S}$-linear codes (resp. $\mathtt{R}$-linear codes) of length ℓ. There are two classical constructions that allow us to build an element of $\mathscr{L}(\mathtt{R}^\ell)$ from an element $\mathscr{B}$ of $\mathscr{L}(\mathtt{S}^\ell)$. One is the *restriction code* of $\mathscr{B}$ which is defined as $\mathtt{Res}_{\mathtt{R}}(\mathscr{B}) := \mathscr{B} \cap \mathtt{R}^\ell$. The second one is based on the fact that the trace map $\mathtt{Tr}_{\mathtt{R}}^{\mathtt{S}} = \sum_{\sigma \in G} \sigma$ is a linear form, therefore it follows that

$$\mathtt{Tr}_{\mathtt{R}}^{\mathtt{S}}(\mathscr{B}) := \left\{ (\mathtt{Tr}_{\mathtt{R}}^{\mathtt{S}}(c_1), \cdots, \mathtt{Tr}_{\mathtt{R}}^{\mathtt{S}}(c_\ell)) \,|\, (c_1, \cdots, c_\ell) \in \mathscr{B} \right\}, \tag{1}$$

is an $\mathtt{R}$-linear code. The relation between the trace code and the restriction code will be given by a generalization of the celebrated result due to Delsarte [2]

$$\mathtt{Tr}_{\mathtt{R}}^{\mathtt{S}}(\mathscr{B}^{\perp_{\varphi'}}) = \mathtt{Res}_{\mathtt{R}}(\mathscr{B})^{\perp_{\varphi}}, \tag{2}$$

where $\perp_\varphi$ and $\perp_{\varphi'}$ denote the duality operators associated to the nondegenerate bilinear forms $\varphi : \mathtt{R}^\ell \times \mathtt{R}^\ell \to \mathtt{R}$ and $\varphi' : \mathtt{S}^\ell \times \mathtt{S}^\ell \to \mathtt{S}$ respectively defined as follows. Let be $\mathbf{a}$ and $\mathbf{b}$ in $\mathtt{S}^\ell$, their Euclidian inner product is defined as $(\mathbf{a},\mathbf{b})_{\mathtt{E}} = a_1 b_1 + a_2 b_2 + \cdots + a_\ell b_\ell$, and if m is even their Hermitian inner product is defined as $(\mathbf{a},\mathbf{b})_{\mathtt{H}} = (\sigma^{\frac{m}{2}}(\mathbf{a}),\mathbf{b})_{\mathtt{E}}$. Note that $(-,-)_{\mathtt{E}}$ is a nondegenerate symmetry bilinear form.
For all $\mathbf{a}$ in $\mathtt{S}^\ell$ and $\mathbf{b}$ in $\mathtt{R}^\ell$, $\mathtt{Tr}_{\mathtt{R}}^{\mathtt{S}}((\mathbf{a},\mathbf{b})_{\mathtt{E}}) = \left(\mathtt{Tr}_{\mathtt{R}}^{\mathtt{S}}(\mathbf{a}),\mathbf{b}\right)_{\mathtt{E}}$, and if m is even, $\mathtt{Tr}_{\mathtt{R}}^{\mathtt{S}}((\mathbf{a},\mathbf{b})_{\mathtt{H}}) = \mathtt{Tr}_{\mathtt{R}}^{\mathtt{S}}((\mathbf{a},\mathbf{b})_{\mathtt{E}})$, since $\mathtt{Tr}_{\mathtt{R}}^{\mathtt{S}}\left(\sigma^{\frac{m}{2}}(\mathbf{a})\right) = \mathtt{Tr}_{\mathtt{R}}^{\mathtt{S}}(\mathbf{a})$. Throughout the paper $\varphi = (-,-)_{\mathtt{E}}$ and if m is even $\varphi' = (-,-)_{\mathtt{H}}$, otherwise $\varphi' = (-,-)_{\mathtt{E}}$. It is clear that

$$\varphi(\mathbf{b}, \mathtt{Tr}_{\mathtt{R}}^{\mathtt{S}}(\mathbf{a})) = \varphi(\mathtt{Tr}_{\mathtt{R}}^{\mathtt{S}}(\mathbf{a}), \mathbf{b}) = \mathtt{Tr}_{\mathtt{R}}^{\mathtt{S}}(\varphi'(\mathbf{a},\mathbf{b})), \text{ for all } \mathbf{a} \in \mathtt{S}^\ell \text{ and } \mathbf{b} \in \mathtt{R}^\ell. \tag{3}$$

A finite commutative ring $\mathtt{R}$ with identity is called a *finite chain ring* if its ideals are linearly ordered by inclusion $\mathtt{R}$ form a chain $\mathtt{R} \supsetneq \mathtt{R}\theta \supsetneq \cdots \supsetneq \mathtt{R}\theta^{s-1} \supsetneq \mathtt{R}\theta^s = \{0\}$. The set $\Gamma(\mathtt{R}) = \Gamma(\mathtt{R})^* \cup \{0\}$ is a complete set of representatives of $\mathtt{R}$ modulo θ and each element a of $\mathtt{R}$ can be expressed uniquely as a *θ-adic decomposition* $a = \gamma_0(a) + \gamma_1(a)\theta + \cdots + \gamma_{s-1}(a)\theta^{s-1}$. Therefore we have a *valuation function* of $\mathtt{R}$, defined by $\vartheta_{\mathtt{R}}(a) := \mathtt{min}\{t \in \{0,1,\cdots,s\} \,|\, \gamma_t(a) \neq 0\}$ and a *degree function* of

$\mathtt{R}$, defined by $\deg_{\mathtt{R}}(a) := \max\{t \in \{0,1,\cdots,s\} \mid \gamma_t(a) \neq 0\}$, for each a in $\mathtt{R}$. We will assume that $\vartheta_{\mathtt{R}}(0) = s$ and $\deg_{\mathtt{R}}(0) = -\infty$.

An *R-linear code* of length ℓ is a $\mathtt{R}$-submodule of $\mathtt{R}^{\ell}$, and the elements of $\mathscr{B}$ are called *codewords*. From now on we will assume that all codes are of length ℓ unless stated otherwise.

Let $\mathtt{R}$ and $\mathtt{S}$ be two finite chain rings with residue fields $\mathbb{F}_q$ and $\mathbb{F}_{q^m}$ respectively. We say that $\mathtt{S}$ is an *extension* of $\mathtt{R}$ and we denote it by $\mathtt{S}|\mathtt{R}$ if $\mathtt{R} \subseteq \mathtt{S}$ and $1_{\mathtt{R}} = 1_{\mathtt{S}}$. $\mathtt{Aut}_{\mathtt{R}}(\mathtt{S})$ will denote the group of automorphisms of $\mathtt{S}$ which fix the elements of $\mathtt{R}$. Note that the map $\sigma : a \mapsto \sum_{t=0}^{s-1} \gamma_t(a)^q \theta^t$ for all $a \in \mathtt{S}$, is in $\mathtt{Aut}_{\mathtt{R}}(\mathtt{S})$ and throughout of this paper G will be the subgroup of $\mathtt{Aut}_{\mathtt{R}}(\mathtt{S})$ generated by σ. For each subgroup H of G one can define the *fixed ring* of H in $\mathtt{S}$ as

$$\mathtt{Fix}_{\mathtt{S}}(H) := \left\{ a \in \mathtt{S} \;\middle|\; \rho(a) = a, \text{ for all } \rho \in H \right\}.$$

Definition 1 *The ring $\mathtt{S}$ is a* Galois extension *of $\mathtt{R}$ with Galois group G if*

1. $\mathtt{Fix}_{\mathtt{S}}(G) = \mathtt{R}$ *and*
2. *there are elements $\alpha_0, \alpha_1, \cdots, \alpha_{m-1}; \alpha_0^*, \alpha_1^*, \cdots, \alpha_{m-1}^*$ in $\mathtt{S}$ such that*

$$\sum_{t=0}^{m-1} \sigma^i(\alpha_t)\sigma^j(\alpha_t^*) = \delta_{i,j},$$

for all $i, j = 0, 1, \cdots, |G| - 1$ (where $\delta_{i,j} = 1_{\mathtt{S}}$ if $i = j$, and $0_{\mathtt{S}}$ otherwise).

Let A be a matrix in $\mathtt{S}^{k \times \ell}$ and $A[i:]$ the i-th row of A; $A[:j]$ the j-th column of A; $A[i;j]$ the (i,j)-entry of A.

1. The *valuation function* of A is the mapping $\vartheta_A : \{1,\cdots,k\} \to \{0,1,\cdots,s\}$, defined by

$$\vartheta_A(i) := \vartheta_{\mathtt{S}}(A[i:]) := \min\{\vartheta_{\mathtt{S}}(A[i;j]) \mid 1 \leq j \leq \ell\}.$$

2. The *pivot* of a nonzero row $A[i:]$ of A, is the first entry among all the entries least with valuation in that row. By convention, the pivot of the zero row is its first entry.

3. The *pivot function* of A is the mapping $\rho : \{1,\cdots,k\} \to \{1,\cdots,\ell\}$, defined by

$$\rho(i) := \min\left\{ j \in \{1;\cdots;\ell\} \mid \vartheta_S(A[i;j]) = \vartheta_i \right\}.$$

Note that the pivot of the row $A[i:]$ is the element $A[i,\rho(i)]$. Let ρ be a ring automorphism of $\mathtt{S}$, it is clear that the pivot function and valuation function of the matrices A and $(\rho(A[i;j]))_{\substack{1\le i\le k\\ 1\le j\le \ell}}$ provide the same values.

Definition 2 (Matrix in row standard form) *A matrix $A \in \mathcal{S}^{k\times\ell}$ is in row standard form if it satisfies the following conditions*

1. *The pivot function of A is injective and the valuation function of A is increasing,*
2. *for all $i \in \{1,\cdots,k\}$, there is $\vartheta_i \in \{0,1,\cdots,s-1\}$ such that $A[i;\rho(i)] = \theta^{\vartheta_i}$ and $A[i:] \in (\theta^{\vartheta_i}\mathcal{S})^{\ell}$ and*
3. *for all pairs $i,t \in \{1,\cdots,k\}$ such that $t \neq i$, then either $i > t$ and $\mathtt{deg}_R(A[t;\rho(i)]) < \vartheta_i$ or $A[i;\rho(t)] = 0$.*

Let $A \in \mathtt{S}^{k\times\ell}$ be a nonzero matrix, we say that a matrix $B \in \mathtt{S}^{k\times\ell}$ is the *row standard form* of A if B is in row standard form and B is row-equivalent to A. Since the set of all generator matrices of any $\mathtt{S}$-linear code $\mathscr{B}$ is a coset under row equivalence, it follows that $\mathscr{B}$ has a unique generator matrix in row standard form that will be denoted by $\mathtt{RSF}(\mathscr{B})$. As usual we define the type of a linear code as follows. Let $\mathscr{B}$ be an $\mathtt{S}$-linear code of length ℓ. Denoted by θ^{ϑ_i} the i-th pivot of $\mathtt{RSF}(\mathscr{B})$. The *type* $\mathscr{B}$ is the $(s+1)$-tuples $(\ell;k_0,k_1,\cdots,k_{s-1})$ where $k_t := |\{\vartheta_i \,|\, \vartheta_i = t\}|$. Clearly the $\mathtt{S}$-rank of $\mathscr{B}$ and the number of codewords of $\mathscr{B}$, are

$$\mathtt{rank}_{\mathtt{S}}(\mathscr{B}) = \sum_{t=0}^{s-1} k_t, \quad \text{and} \quad |\mathscr{B}| = q^{m\left(\sum_{t=0}^{s-1} k_t(s-t)\right)}.$$

Let $\mathtt{S}|\mathtt{R}$ be a Galois extension of finite chain ring with Galois group G. The Galois group G acts on $\mathscr{L}(\mathtt{S}^{\ell})$ as follows; Let $\mathscr{B}$ in $\mathscr{L}(\mathtt{S}^{\ell})$ and σ in G

$$\sigma(\mathscr{B}) = \left\{ (\sigma(c_0),\sigma(c_1),\cdots,\sigma(c_{\ell-1})) \,\middle|\, (c_0,c_1,\cdots,c_{\ell-1}) \in \mathscr{B} \right\}. \tag{4}$$

A linear code $\mathscr{B}$ over $\mathtt{S}$ is called *Galois invariant* if $\sigma(\mathscr{B}) = \mathscr{B}$ for all $\sigma \in G$.

Theorem 3 *Let $\mathscr{B}$ be an $\mathcal{S}$-linear code and $A \in \mathcal{S}^{k\times\ell}$ a generator matrix of $\mathscr{B}$. Then the following facts are equivalent.*

1. *$\mathscr{B}$ is Galois invariant.*
2. *$\mathtt{RSF}(\mathscr{B})$ in $\mathcal{R}^{k\times\ell}$.*

Corollary 1 *Let $\mathscr{B}$ be a linear code over $\mathtt{S}$, $\mathscr{B}$ is Galois invariant if and only if $\mathtt{RSF}(\mathscr{B}) = \mathtt{RSF}(\mathtt{Res}(\mathscr{B}))$.*

Corollary 2 *Let $\mathscr{B}$ be a linear code over $\mathtt{S}$ of the type $(\ell; k_0, k_1, \cdots, k_{s-1})$. Then the following conditions are equivalent.*

1. *$\mathscr{B}$ is Galois invariant,*
2. *$\mathtt{Res}_R(\mathscr{B})$ is of type $(\ell; k_0, k_1, \cdots, k_{s-1})$.*

For all $\mathscr{B}_1, \mathscr{B}_2 \in \mathscr{L}(\mathtt{S}^\ell)$, $\mathscr{B}_1 \vee \mathscr{B}_2 = \mathscr{B}_1 + \mathscr{B}_2$ is the smallest $\mathtt{S}$-linear code containing $\mathscr{B}_1$ and $\mathscr{B}_2$, note that $\left(\mathscr{L}(\mathtt{S}^\ell); \cap, \vee\right)$ is a lattice. Let $\mathscr{E}$ be a subset of $\mathtt{S}^\ell$, we define the *extension code* of $\mathscr{E}$ to $\mathtt{S}$, denoted $\mathtt{Ext}(\mathscr{E})$, as the code form by all $\mathtt{S}$-linear combinations of elements in $\mathscr{E}$.

Proposition 1 *The operators*

$$\mathscr{L}(\mathtt{S}^\ell) \underset{\mathtt{Ext}}{\overset{\mathtt{Tr}_R^S;\mathtt{Res}_R}{\rightleftarrows}} \mathscr{L}_\ell(R) \tag{5}$$

are lattice morphisms. Moreover,

$\mathtt{Ext}(\mathscr{C}^\perp) = \mathtt{Ext}(\mathscr{C})^\perp$ *and* $\mathtt{Tr}_R^S(\mathtt{Ext}(\mathscr{C})) = \mathtt{Res}_R(\mathtt{Ext}(\mathscr{C})) = \mathscr{C}$ *for all* $\mathscr{C} \in \mathscr{L}_\ell(R)$.

Definition 4 (Galois closure and Galois interior) *Let $\mathscr{B}$ be a linear code over $\mathtt{S}$.*

1. *The* Galois closure *of $\mathscr{B}$, denoted by $\widetilde{\mathscr{B}}$, is the smallest linear code over $\mathtt{S}$, containing $\mathscr{B}$, which is Galois invariant,*

$$\widetilde{\mathscr{B}} := \bigcap \left\{ \mathscr{T} \in \mathscr{L}(\mathtt{S}^\ell) \;\middle|\; \mathscr{T} \subseteq \mathscr{B} \text{ and } \mathscr{T} \text{ Galois invariant} \right\}.$$

2. *The* Galois interior *of $\mathscr{B}$, denoted $\overset{\circ}{\mathscr{B}}$, is the greatest $\mathtt{S}$-linear subcode of $\mathscr{B}$, which is Galois invariant,*

$$\overset{\circ}{\mathscr{B}} := \bigvee \left\{ \mathscr{T} \in \mathscr{L}(\mathtt{S}^\ell) \;\middle|\; \mathscr{T} \supseteq \mathscr{B} \text{ and } \mathscr{T} \text{ Galois invariant} \right\}.$$

A map $\mathtt{J}_G : \mathscr{L}(\mathtt{S}^\ell) \to \mathscr{L}(\mathtt{S}^\ell)$ is called a *Galois operator* if $\mathtt{J}_G$ is an morphism of lattices such that

1. $\mathtt{J}_G(\mathtt{J}_G(\mathscr{B})) = \mathtt{J}_G(\mathscr{B})$ and

2. for all $\mathscr{B}$ in $\mathscr{L}(\mathtt{S}^\ell)$ the code $\mathtt{J}_G(\mathscr{B})$ is Galois invariant.

The Galois closure and Galois interior are indeed Galois operators and $\overset{\sim}{\overset{\circ}{\mathscr{B}}} = \overset{\circ}{\mathscr{B}}$, $\overset{\circ}{\widetilde{\mathscr{B}}} = \widetilde{\mathscr{B}}$. From Definition 4, it follows that $\mathscr{B}$ is Galois invariant if and only if $\widetilde{\mathscr{B}} = \overset{\circ}{\mathscr{B}}$.

Proposition 2 *If $\mathscr{B}$ is a linear code over $\mathtt{S}$ then* $\left(\overset{\circ}{\mathscr{B}^\perp}\right) = \left(\widetilde{\mathscr{B}}\right)^\perp$.

Lemma 5 *Let $\mathscr{B}$ be a linear code over $\mathtt{S}$. Then* $\overset{\circ}{\mathscr{B}} = \mathtt{Ext}(\mathtt{Res}_R(\mathscr{B})) = \bigcap_{\sigma\in G} \sigma(\mathscr{B})$.

For any $\mathscr{B}$ in $\mathscr{L}\left(\mathtt{S}^\ell\right)$, we consider $\mathscr{L}(\mathscr{B})$ the lattice of $\mathtt{S}$-linear subcode of $\mathscr{B}$. Let us define

$$\begin{array}{rccc} \mathtt{Stab}: & \mathscr{L}(\mathscr{B}) & \to & \mathtt{Sub}(G) \\ & \mathscr{T} & \mapsto & \mathtt{Stab}(\mathscr{T}), \end{array} \quad \text{and} \quad \begin{array}{rccc} \mathtt{Fix}_{\mathscr{B}}: & \mathtt{Sub}(G) & \to & \mathscr{L}(\mathscr{B}) \\ & H & \mapsto & \bigcap_{\sigma\in H}\sigma(\mathscr{B}), \end{array}$$

where $\mathtt{Stab}(\mathscr{T}) = \left\{ \sigma \in G \,\middle|\, \sigma(\mathbf{c}) = \mathbf{c}, \text{ for all } \mathbf{c} \in \mathscr{T} \right\}$.

Let H a subgroup of G, we say that $\mathscr{B}$ is H-invariant if $\mathtt{Fix}_{\mathscr{B}}(H) = \mathscr{B}$. Note that $\mathtt{Fix}_{\mathscr{B}}(H)$ is an H-interior of $\mathscr{B}$. From Lemma 5 it follows that

$$\mathtt{Fix}_{\mathscr{B}}(H) = \mathtt{Ext}(\mathtt{Res}_{\mathtt{T}}(\mathscr{B})),$$

where $\mathtt{T} = \mathtt{Fix}_{\mathtt{S}}(H)$. Moreover $\mathtt{Fix}_{\mathscr{B}}(\mathtt{Stab}(\mathscr{B})) = \mathscr{B}$ and $\mathtt{Stab}(\mathtt{Fix}_{\mathscr{B}}(H)) = H$. Therefore we have a Galois correspondence on $\mathscr{L}(\mathscr{B})$ as follows.

Theorem 6 *For each $\mathscr{B}$ in $\mathscr{L}\left(\mathtt{S}^\ell\right)$, the pair $(\mathtt{Stab}; \mathtt{Fix}_{\mathscr{B}})$ is a Galois correspondence between $\mathscr{B}$ and G.*

References

[1] Bierbrauer, J. *The Theory of Cyclic Codes and a Generalization to Additive Codes.* Des. Codes Cryptography 25(2): 189-206 (2002)

[2] Delsarte, P. *On subfield subcodes of modified Reed-Solomon codes*, IEEE Trans. Inform. Theory IT-21 (5) (1975)

[3] Martinez-Moro E., Nicolas A.P.,Rua F.,*On trace codes and Galois invariance over finite commutative chain rings*, Finite Fields Appl. Vol. 22, pp. 114-121 (2013).

[4] McDonald B. R., *Finite Rings with Identity*, Marcel Dekker, New York (1974).

[5] Norton G.H., Salagean A., *On the Structure of Linear and Cyclic Codes over a Finite Chain Ring*, AAECC Vol. 10, pp. 489-506, (2000).

Betti Numbers and Generalized Hamming Weights

Irene Márquez-Corbella and Edgar Martínez-Moro

Dept. of Mathematics, Statistics and O. Research, University of La Laguna, Spain.
irene.marquez.corbella@ull.es
Institute of Mathematics, University of Valladolid, Spain. Edgar.Martinez@uva.es

We can associate to each linear code $\mathscr{C}$ defined over a finite field the matroid $M[H]$ of its parity check matrix H. For any matroid M one can define its generalized Hamming weights which are the same as those of the code $\mathscr{C}$. In [2] the authors show that the generalized Hamming weights of a matroid are determined by the $\mathbb{N}$-graded Betti numbers of the Stanley-Reisner ring of the simplicial complex whose faces are the independent set of M. In this talk we go a step further. Our practical results indicate that the generalized Hamming weights of a linear code $\mathscr{C}$ can be obtained from the monomial ideal associated with a test-set for $\mathscr{C}$. Moreover, recall that in [3] we use the Gröbner representation of a linear code $\mathscr{C}$ to provide a test-set for $\mathscr{C}$.

Our results are still a work in progress, but its applications to Coding Theory and Cryptography are of great value.

1 Notation and Prerequisites

We begin with an introduction of basic definitions and some known results. By $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{F}_q$ (where q is a primer power) we denote the set of positive integers, the set of integers and the finite field with q elements, respectively.

Definition 1 *A matroid M is a pair (E,I) consisting of a finite set E called ground set and a collection I of subsets of E called independent sets, satisfying the following conditions:*

1. *The empty set is independent, i.e. $\emptyset \in I$*
2. *If $A \in I$ and $B \subset A$, then $B \in I$*
3. *If $A,B \in I$ and $|A| < |B|$, then there exists $e \in B \setminus A$ such that $A \cup \{e\} \in I$*

Let $M = (E,I)$ be a matroid. A maximal independent subset of E is called a *basis* of M. A direct consequence of the previous definition is that all bases of M have the same cardinality. Thus, we define the *rank* of the matroid M as the cardinality of any basis of M, denoted by $\text{rank}(M)$. A subset E that does not belong

to I is called *dependent set*. Minimal dependent subsets of E are known as *circuits* of M. A set is said to be a *cycle* if it is a disjoint union of circuits. The collection of cycles of M is denoted by $\mathscr{C}(M)$. For all $\sigma \in E$, the *nulity function* of σ is given by $n(\sigma) := |\sigma| - \text{rank}(M_\sigma)$ with $\text{rank}(M_\sigma) = \max\{|A| \mid A \in I \text{ and } A \subset \sigma\}$, i.e. the restriction of $\text{rank}(M)$ to the subsets of σ.

Let us consider an $m \times n$ matrix A in $\mathbb{F}_q$ whose columns are indexed by $E = \{1,\ldots,n\}$ and take I to be the collection of subsets J of E for which the column vectors $\{A_j \mid j \in J\}$ are linearly independent over $\mathbb{F}_q$. Then (E,I) defines a matroid denoted by $M[A]$. A matroid $M = (E,I)$ is $\mathbb{F}_q$-representable if it is isomorphic to $M[A]$ for some $A \in \mathbb{F}_q^{m\times n}$. Then the matrix A is called the representation matrix of M. The following well known results describes the relation between the colleciton of all cycles of a matroid M and its representation matrix.

Proposition 1 *Let $M = (E,I)$ be a $\mathbb{F}_q$-representable matroid. Then $\mathscr{C}(M)$ is the null space of a representation matrix of M. Furthermore, the dimension of $\mathscr{C}(M)$ is $|E| - \text{rank}(M)$.*

Let Δ be a simplicial complex on the finite ground set E. Let $\mathbb{K}$ be a field and let $\mathbf{x}$ be the indeterminates $\mathbf{x} = \{x_e \mid e \in E\}$. The *Stanley-Reisner* ideal of Δ is, by definition,

$$I_\Delta = \langle \mathbf{x}^\sigma \mid \sigma \notin \Delta \rangle$$

The *Stanley-Reisner ring* of I_Δ, denoted by R_Δ, is defined to be the quotient ring $R_\Delta = \frac{\mathbb{K}[\mathbf{x}]}{I_\Delta}$. This ring has a minimal free resolution as $\mathbb{N}^E$-graded module:

$$0 \longleftarrow R_\Delta \longleftarrow P_0 \longleftarrow P_1 \longleftarrow \cdots \longleftarrow P_l \longleftarrow 0$$

where each P_i is given by $P_i = \bigoplus_{\alpha\in\mathbb{N}^E} \mathbb{K}[\mathbf{x}](-\alpha)^{\beta_{i,\alpha}}$. We write $\beta_{i,\alpha}$ for the $\mathbb{N}^E$-graded Betti Numbers of Δ.

1.1 Matroids and Simplicial complex

A matroid $M = (E,I)$ is a simplicial complex whose faces are the independent sets. Thus, $I_M := \langle \mathbf{x}^\sigma \mid \sigma \in \mathscr{C} \rangle$ where $\mathscr{C}$ is the set of all circuits of M. Define $N_i = \{\sigma \in N \mid n(\sigma) = d\}$.

Theorem 1 ([2]Theorem 1) *Let M be a matroid on the ground set E. Let $\sigma \subset E$. Then, $\beta_{i,\sigma} \neq 0$ if and only if σ is minimal in N_i.*

Definition 2 *Let $M = (E,I)$ be a matroid, we define the generalized Hamming weights of M to be $d_i = \min\{|\sigma| \mid n(\sigma) = i\}$.*

Corollary 1 *Let M be a matroid on the ground set E. Then,*

$$d_i = \min\{d \mid \beta_{i,d} \neq 0 \quad \textit{for all} \quad 1 \leq i \leq |E| - \text{rank}(M)\}.$$

1.2 Matroids and linear codes

An $[n,k]_q$ linear code $\mathscr{C}$ is a k-dimensional subspace of $\mathbb{F}_q^n$. We define a *generator matrix* of $\mathscr{C}$ to be a $k \times n$ matrix G whose row vectors span $\mathscr{C}$, while a *parity check matrix* of $\mathscr{C}$ is an $(n-k) \times n$ matrix H whose null space is $\mathscr{C}$.

Let us denote by $\mathrm{d}_H(\cdot,\cdot)$ and $\mathrm{w}_H(\cdot)$ the *Hamming distance* and the *Hamming weight* on $\mathbb{F}_q^n$, respectively. We write d for the *minimum Hamming distance* of the code $\mathscr{C}$, which is equal to its minimum weight. Thus, the error correcting capability of $\mathscr{C}$ is $t = \left\lfloor \frac{d-1}{2} \right\rfloor$ where $\lfloor \cdot \rfloor$ is the greatest integer function. For every codeword $\mathbf{c} \in \mathscr{C}$ its *support*, $\mathrm{supp}(\mathbf{c})$, is defined as its support as a vector in $\mathbb{F}_q^n$, i.e. $\mathrm{supp}(\mathbf{c}) = \{i \mid c_i \neq 0\}$. We will denote by $\mathscr{M}_{\mathscr{C}}$ the set of codewords of minimal support of $\mathscr{C}$.

A *test-set* $\mathscr{T}_{\mathscr{C}}$ for $\mathscr{C}$ is a set of codewords such that for every word $\mathbf{y} \in \mathbb{F}_q^n$, either $\mathbf{y}$ belongs to the set of coset leaders, or there exists an element $\mathbf{t} \in \mathscr{T}_{\mathscr{C}}$ such that $\mathrm{w}_H(\mathbf{y}-\mathbf{t}) < \mathrm{w}_H(\mathbf{y})$.

Definition 3 *The r^{th} generalized Hamming weight of $\mathscr{C}$ denoted by $d_r(\mathscr{C})$ is the smallest support of an r-dimensional subcode of $\mathscr{C}$. That is,*

$$d_r(\mathscr{C}) = \min\{\mathrm{supp}(D) \mid D \subseteq \mathscr{C} \text{ and } \mathrm{rank}(D) = r\}$$

In [3] the authors associate a binomial ideal to an arbitrary linear code provided by the rows of a generator matrix and the relations given by the additive table of the defining field.

Let $\mathbf{X}$ denote n vector variables $X_1,\ldots,X_n$ such that each variable X_i can be decomposed into $q-1$ components $x_{i,1},\ldots,x_{i,q-1}$ with $i = 1,\ldots,n$. A monomial in $\mathbf{X}$ is a product of the form:

$$\mathbf{X}^{\mathbf{u}} = X_1^{\mathbf{u}_1} \cdots \mathbf{X}_n^{\mathbf{u}_n} = \left(x_{1,1}^{u_{1,1}} \cdots x_{1,q-1}^{u_{1,q-1}}\right) \cdots \left(x_{n,1}^{u_{n,1}} \cdots x_{n,q-1}^{u_{n,q-1}}\right)$$

where $\mathbf{u} \in \mathbb{Z}_{\geq 0}^{n(q-1)}$. The total degree of $\mathbf{X}^{\mathbf{u}}$ is the sum $\deg(\mathbf{X}^{\mathbf{u}}) = \sum_{i=1}^{n}\sum_{j=1}^{q-1} u_{i,j}$. When $\mathbf{u} = (0,\ldots,0)$, note that $\mathbf{X}^{\mathbf{u}} = 1$. Then, the polynomial ring $\mathbb{K}[\mathbf{X}]$ is the set of all polynomials in $\mathbf{X}$ with coefficients in $\mathbb{K}$.

Recall that the multiplicative group $\mathbb{F}_q^*$ of nonzero elements of $\mathbb{F}_q$ is cyclic. A generator of the cyclic group $\mathbb{F}_q^*$ is called a primitive element of $\mathbb{F}_q$, i.e. $\mathbb{F}_q$ consist of 0 and all powers from 1 to $q-1$ of that primitive element. Let α be a primitive element of $\mathbb{F}_q$. We define by $\mathscr{R}_{X_i}$, the set of all the binomials on the variables X_i associated to the relations given by the additive table of the field $\mathbb{F}_q = \langle \alpha^j \mid j = 1,\ldots,q-1\rangle \cup \{0\}$, i.e.

$$\mathscr{R}_{X_i} = \left\{ \ \{x_{i,u}x_{i,v} - x_{i,w} \mid \alpha^u + \alpha^v = \alpha^w\} \quad \cup \quad \{x_{i,u}x_{i,v} - 1 \mid \alpha^u + \alpha^v = 0\} \ \right\}$$

with $i = 1, \ldots, n$. Note that there are $\binom{q}{2}$ different binomials in $\mathscr{R}_{X_i}$. We define $\mathscr{R}_{\mathbf{X}}$ as the ideal generated by the union of all binomial ideals $\mathscr{R}_{X_i}$, i.e. $\mathscr{R}_{\mathbf{X}} = \left\langle \cup_{i=1}^{n} \mathscr{R}_{X_i} \right\rangle$

We will use the following characteristic crossing functions. These applications aim at describing a one-to-one correspondence between the finite field $\mathbb{F}_q$ with q elements and the standard basis of $\mathbb{Z}^{q-1}$, denoted as $E_q = \{\mathbf{e}_1, \ldots, \mathbf{e}_{q-z}\}$ where $\mathbf{e}_i$ is the unit vector with a 1 in the i-th coordinate and 0's elsewhere.

$$\Delta: \quad \mathbb{F}_q \quad \longrightarrow \quad E_q \cup \{\mathbf{0}\} \subseteq \mathbb{Z}^{q-1} \qquad \text{and} \qquad \nabla: \quad E_q \cup \{\mathbf{0}\} \quad \longrightarrow \quad \mathbb{F}_q$$

1. The map Δ replaces the element $\mathbf{a} = \alpha^i \in \mathbb{F}_q$ by the vector $\mathbf{e}_i$ and $0 \in \mathbb{F}_q$ by the zero vector $\mathbf{0} \in \mathbb{Z}^{q-1}$.

2. The map ∇ recovers the element $\alpha^j \in \mathbb{F}_q$ from the unit vector $\mathbf{e}_j$ and the zero element $0 \in \mathbb{F}_q$ from the zero vector $\mathbf{0} \in \mathbb{Z}^{q-1}$.

These maps will be used with matrices and vectors acting coordinate-wise. Although Δ is not a linear function. Note that we have:

$$\mathbf{X}^{\Delta \mathbf{a}} \cdot \mathbf{X}^{\Delta \mathbf{b}} = \mathbf{X}^{\Delta \mathbf{a} + \Delta \mathbf{b}} = \mathbf{X}^{\Delta(\mathbf{a}+\mathbf{b})} \mod \mathscr{R}_{\mathbf{X}} \text{ for all } \mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n.$$

Let $\mathscr{C}$ be an $[n,k]_q$ linear code. We define the *ideal associated* to $\mathscr{C}$ as the binomial ideal:

$$I(\mathscr{C}) = \left\langle \left\{ \mathbf{X}^{\Delta \mathbf{a}} - \mathbf{X}^{\Delta \mathbf{b}} \mid \mathbf{a} - \mathbf{b} \in \mathscr{C} \right\} \right\rangle \subseteq \mathbb{K}[\mathbf{X}]$$

Given the rows of a generator matrix $\mathscr{C}$, labelled by $\{\mathbf{w}_1, \ldots, \mathbf{w}_k\} \subseteq \mathbb{F}_q^n$, we define the following ideal:

$$I_+(\mathscr{C}) = \left\langle \left\{ \mathbf{X}^{\Delta(\alpha^j \mathbf{w}_i)} - 1 \right\}_{\substack{i=1,\ldots,n \\ j=1,\ldots q-1}} \cup \left\{ \mathscr{R}_{X_i} \right\}_{i=1,\ldots,n} \right\rangle \subseteq \mathbb{K}[\mathbf{X}]$$

Theorem 2 *[3][Theorem 2.3]* $I(\mathscr{C}) = I_+(\mathscr{C})$

Remark 1 *In the binary case, given a generator matrix $G \in \mathbb{F}_2^{k \times n}$ of an $[n,k]_2$-code $\mathscr{C}$ and let label its rows by $\{\mathbf{w}_1, \ldots, \mathbf{w}_k\} \subseteq \mathbb{F}_2^n$. We define the ideal associated to $\mathscr{C}$ as the binomial ideal:*

$$I_+(\mathscr{C}) = \left\langle \left\{ \mathbf{X}^{\mathbf{w}_i} - 1 \right\}_{i=1,\ldots,k} \cup \left\{ x_i^2 - 1 \right\}_{i=1,\ldots,n} \right\rangle \subseteq \mathbb{K}[\mathbf{X}]$$

Now, let $\mathscr{G} = \{g_1, \ldots, g_s\}$ be the reduced Gröbner basis of the ideal $I_+(\mathscr{C})$ with respect to $\succ$, where we take $\succ$ to be any degree compatible ordering on $\mathbb{K}[\mathbf{X}]$ with

$X_1 \prec \ldots \prec X_n$. By Lemma [3][Lemma 3.3] we know that all elements of $\mathscr{G} \setminus \mathscr{R}_{\mathbf{X}}$ are in standard form, so for $g_i \in \mathscr{G} \setminus \mathscr{R}_{\mathbf{X}}$ with $i = 1, \ldots, s$, we define

$$g_i = \mathbf{X}^{\Delta \mathbf{g}_i^+} - \mathbf{X}^{\Delta \mathbf{g}_i^-} \quad \text{with} \quad \mathbf{X}^{\Delta \mathbf{g}_i^+} \succ \mathbf{X}^{\Delta \mathbf{g}_i^-} \quad \text{and} \quad \mathbf{g}_i^+ - \mathbf{g}_i^- \in \mathscr{C}.$$

Using [3][Proposition 4], we know that the set $\mathscr{T} = \left\{ \mathbf{g}_i^+ - \mathbf{g}_i^- \mid i = 1, \ldots, s \right\}$ is a test-set for $\mathscr{C}$.

Example 1 *Consider the* $[6,3,2]_2$ *binary code* $\mathscr{C}$ *defined by the following generator matrix:*

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix} \in \mathbb{F}_2^{3 \times 6}$$

Let us label the rows of G by $\mathbf{w}_1$ *and* $\mathbf{w}_2$*. By the previous theorem, the ideal associated to the linear code* $\mathscr{C}$ *may be defined as the following ideal:*

$$\begin{aligned} I_+(\mathscr{C}) &= \left\langle \ \{\mathbf{X}^{\mathbf{w}_i} - 1\}_{i=1,2} \ \cup \ \{\mathscr{R}_{X_i}\}_{i=1,\ldots,6} \ \right\rangle \\ &= \left\langle \ \left\{ \begin{array}{c} x_1 x_6 - 1 \\ x_2 x_3 x_5 - 1 \\ x_4 x_5 x_6 - 1 \end{array} \right\} \ \cup \ \left\{ x_i^2 - 1 \right\}_{i=1,\ldots,6} \ \right\rangle \end{aligned}$$

If we compute a reduced Gröbner basis $\mathscr{G}$ *of* $I_+(\mathscr{C})$ *we obtained a test-set consisting of* 4 *codewords:*

$$\mathscr{T}_{\mathscr{C}} = \{(1,0,0,0,0,1),(0,1,1,0,1,0),(0,1,1,1,1,0,1),(0,0,0,1,1,1)\}$$

For fuller discussion of this algebraic structure see [4, 1] and the references therein.

The connection between linear codes and matroids will turn out to be fundamental for the development of the subsequent results. Thus, a brief review will be provided here.

Given an $m \times n$ matrix H in $\mathbb{F}_q$, then H can be seen not only as the representation matrix of the $\mathbb{F}_q$-representable matroid $M[H]$ but also as a parity check matrix of an $[n,k]$-code $\mathscr{C}$. Furthermore, there exists a one to one correspondence between $\mathbb{F}_q$-representable matroids and linear codes, since for any $H, H' \in \mathbb{F}_q^{m \times n}$, $M[H] = M[H']$ if an only if H and H' are parity check matrices of the same code $\mathscr{C}$. This association enables us to work with $\mathbb{F}_q$-representable matroids and linear codes as if they were the same object and thus we can conclude some properties of linear codes using tools from matroid theory and vice-versa.

2 Our Conjecture

Let $M = (E, I)$ be a matroid and $\mathscr{C}$ be the set of all circuits of M. Consider $\mathscr{T}$ a collection of cycles of M with the following property: $\bigcup_{\tau\in\mathscr{C}} \tau = \bigcup_{\tau\in\mathscr{T}} \tau$. We define the ideal $I_{\mathscr{T}} = \langle \mathbf{x}^{\sigma} \mid \sigma \in \mathscr{T} \rangle$.

Conjecture 1 *Let $\beta'_{i,\alpha}$ the $\mathbb{N}^E$-graded betti number of $I_{\mathscr{T}}$, related with the minimal free resolution of $R = \frac{\mathbb{K}[X]}{I_{\mathscr{T}}}$ as $\mathbb{N}^E$-graded module. Then, we have a similar result as Theorem 1 and Corollary 1.*

If we talk about linear codes, the conjecture allows us to compute the set of generalized Hamming weight of a linear code $\mathscr{C}$ using a Test-set for $\mathscr{C}$, in other words, by computing a Grobner basis of the ideal associated to $\mathscr{C}$.

Corollary 2 *Let $\mathscr{T}_{\mathscr{C}}$ be a test-set for the linear code $\mathscr{C}$. Consider the monomial ideal: $I_{\mathscr{T}_{\mathscr{C}}} = \langle \mathbf{x}^{\sigma} \mid \sigma \in \mathscr{T}_{\mathscr{C}} \rangle$. Let $\beta'_{i,\alpha}$ the $\mathbb{N}^E$-graded betti numbers of $I_{\mathscr{T}_{\mathscr{C}}}$. Then,*

$$d_i(\mathscr{C}) = \min\left\{ d \mid \beta'_{i,d} \neq 0 \right\} \text{ for } 1 \leq i \leq n-k$$

Example 2 *Now we use the same code of Example 1. In this case the support of a test-set $T_{\mathscr{C}}$ is given by: $\mathscr{T} = \{\{2,3,5\},\{2,3,4,6\},\{4,5,6\},\{1,6\}\}$ i.e. we consider the ideal: $I_{\mathscr{T}} = \langle x_2x_3x_5, x_2x_3x_4x_6, x_4x_5x_6, x_1x_6 \rangle \subseteq \mathbb{K}[x_1,\ldots,x_6]$. We get the Betti diagram*

	1	2	3
1	1		
2	2	1	
3	1	4	2

Thus $\beta'_{1,2}$, $\beta'_{2,4}$ and $\beta'_{3,6}$ are the minimal $\beta'_{i,d} \neq 0$ with $i = 1,2,3$. Or equivalently, $d_1 = 2$, $d_2 = 4$ and $d_3 = 6$.

References

[1] M. Borges-Quintana, M.A. Borges-Trenard, P. FitzPatrick and E. Martínez-Moro. *Gröbner bases and combinatorics for binary codes*. Applicable Algebra in Engineering, Communication and Computing. 19(5): 393-411, 2008.

[2] J. T. Johnsen and H. Verdure. *Hamming weights and Betti numbers of Stanley–Reisner rings associated to matroids*. Applicable Algebra in Engineering, Communication and Computing. 24(1): 73-93, 2013.

[3] I. Márquez-Corbella, E. Martínez-Moro and E. Suárez-Canedo. *On the ideal associated to a linear code*. Advances in Mathematics of Communications (AMC). 10(2): 229-254, 2016.

[4] I. Márquez-Corbella and E. Martínez-Moro. *Algebraic structure of the minimal support codewords set of some linear codes*. Advances in Mathematics of Communications (AMC). 5(2): 233-244, 2011.

S11
SC-Square: Symbolic Computation and Satisfiability Checking

SC^2: Satisfiability Checking meets Symbolic Computation

Erika Ábrahám[1], John Abbott[11], Bernd Becker[2], Anna M. Bigatti[3], Martin Brain[10]. Bruno Buchberger[4], Alessandro Cimatti[5], James H. Davenport[6], Matthew England[7], Pascal Fontaine[8], Stephen Forrest[9], Alberto Griggio[5], Daniel Kroening[10], Werner M. Seiler[11], Thomas Sturm[8,12]

[1] *RWTH Aachen, Aachen, Germany*
[2] *Albert-Ludwigs-Universität, Freiburg, Germany*
[3] *Università degli studi di Genova, Italy*
[4] *Johannes Kepler Universität, Linz, Austria*
[5] *Fondazione Bruno Kessler, Trento, Italy*
[6] *University of Bath, Bath, U.K.*
[7] *Coventry University, Coventry, U.K.*
[8] *LORIA, Inria, Université of Lorraine, Nancy, France*
[9] *Maplesoft Europe Ltd*
[10] *University of Oxford, Oxford, U.K.*
[11] *Universität Kassel, Kassel, Germany*
[12] *Max-Planck-Institut für Informatik, Saarbrücken, Germany*

Symbolic Computation and *Satisfiability Checking* are two research areas, both having their individual scientific focus but sharing also common interests in the development, implementation and application of decision procedures for arithmetic theories. Despite their commonalities, the two communities are rather weakly connected. The aim of our newly accepted SC^{2}project (H2020-FETOPEN-CSA) is to strengthen the connection between these communities by creating common platforms, initiating interaction and exchange, identifying common challenges, and developing a common roadmap from theory along the way to tools and (industrial) applications. In this talk we report on the aims and on the first activities of this project, and formalise some relevant challenges for the unified SC^{2}community. For more details, see `www.sc-square.org/CSA/welcome.html`.

Satisfiability Modulo Theories: Where We Are, How We Got Here, and Where We Could Go Next

M. Brain[1]

[1] *University of Oxford, UK* martin.brain@cs.ox.ac.uk

This talk will introduce the field of Satisfiability Modulo Theories (SMT) from the foundations, along with some of the history and culture of the field. Topics covered will include the SMT-LIB community initiative that ensures interoperability between tools, historic and modern solver architectures, how the demands of software verification have shaped and driven the fields, some of the 'non-traditional' algebras that are of interest and finally what problems need a new generation of ideas and tools.

Integration of a SAT Solver into Maple

S. Forrest[1]

[1] *Maplesoft Europe Ltd., Cambridge, UK,* `sforrest@maplesoft.com`

Maple is a commercial computer algebra system developed and sold since 1988 by Maplesoft [1]. Its most recent major release, in March 2016, featured the augmentation of existing tools for manipulating logical expressions with a link to MiniSat, a high-performing open-source SAT solver [2].

In this talk, we will discuss some design questions and technical issues encountered in the course of implementing this Maple–MiniSat integration, as well as some additional ways Maple might make further use of a SAT oracle and the promise offered by a possible future integration with an SMT solver.

References

[1] *Maple Programming Guide*, Toronto: Maplesoft, a division of Waterloo Maple Inc., 2005–2016.

[2] Niklas Een and Niklas Sorensson, *An Extensible SAT-solver* [extended version 1.2], website `http://minisat.se/downloads/MiniSat.pdf`, (2003).

Implicitization with Groebner Bases: the well known algorithm and algorithms which work

J. Abbott[1], A. M. Bigatti[2], L. Robbiano[2]

[1] *Universität Kassel, abbott@dima.unige.it*
[2] *Università degli Studi di Genova, {bigatti,robbiano}@dima.unige.it*

We present new, practical algorithms for the hypersurface implicitization problem: namely, given a parametric description (in terms of polynomials or rational functions) of the hypersurface, find its implicit equation.

Two of them are for polynomial parametrizations: one algorithm, "ElimTH", has as main step the computation of an elimination ideal via a *truncated, homogeneous* Gröbner basis. The other algorithm, "Direct", computes the implicitization directly using an approach inspired by the generalized Buchberger-Möller algorithm. Either may be used inside the third algorithm, "RatPar", to deal with parametrizations by rational functions.

Finally we show how these algorithms can be used in a modular approach, algorithm "ModImplicit", for avoiding the high costs of arithmetic with rational numbers. We exhibit experimental timings to show the practical efficiency of our new algorithms.

References

[1] J. Abbott, A. M. Bigatti, L. Robbiano
Implicitization of Hypersurfaces , `arXiv:1602.03993` (2016).

Symbolic Computation: give and take for SC2

J. Abbott[1]

[1] *Universität Kassel, Germany* jabbott@mathematik.uni-kassel.de

The aim of the SC^2 project is promote collaboration between researchers in Symbolic Computation and those in Satisfiability Checking. In this talk we shall adopt the perspective of a researcher in Symbolic Computation, and look at aspects of our expertise (both theoretical and practical) which we think are likely to be useful to SC^2, and also at expertise (and challenges) which we hope to acquire from the collaboration. The intent is to identify promising directions rather than "ready-to-eat" solutions; this in preparation for the open discussion session.

One clear challenge is achieving *SMT compliance*. An important point for practical efficiency is *incrementality*: the SMT solver is likely to ask for the satisfiability of many systems which have large subsets of generators in common. Another novel aspect is producing an *explanation* for unsatisfiability: this means determining a small subset which is unsatisfiable, so that the SMT solver can skip large chunks of search space.

Symbolic computation tools likely to be useful (at least in theory) include polynomial factorization, Gröbner bases, cylindrical algebraic decompositions. A significant question will be how the practical efficiency of these techniques contributes to overall computation time (at least on typical example problems).

In the case of a satisfiable system, what sort answer should be returned to the SMT solver? In principle an exact sample point could be determined, but may be an unwieldy set of algebraic numbers; often an "implicit" representation is more compact.

There are also a number of low-level questions such as how to effect communication between the SMT solver's "traversal engine", and the "theory engine", namely the symbolic computation software. We mention also philosophical questions such as the acceptability of probabilistic/heuristic methods (where a significant gain in speed is paid for by allowing a very small chance of error).

S12
General Session

Computation of Hilbert Schemes

M. Albert[1]

[1] *University of Kassel, Germany, albert@mathematik.uni-kassel.de*

Hilbert schemes are a basic topic in Algebraic Geometry [1, 2]. Methods related to Gröbner bases are fundamental here, as Hartshorne's proof of the connectedness of Hilbert schemes via generic initial ideals demonstrates [3]. For many purposes, the explicit construction of Hilbert schemes is important. Classical approaches lead to prohibitively large equations. Newer ideas like Gröbner strata [4, 5] lead to improvements, but do not provide open covers. Despite all advances, it has remained a great challenge to construct Hilbert schemes even for very small Hilbert polynomials.

A novel approach replacing Gröbner bases by J-marked bases [6, 7] was proposed by the group of Margharita Roggero. For every strongly stable ideal J, one obtains here a larger family which corresponds to an open subscheme and which can be described by equations of low degree.

We have implemented several of the new algorithms in the computer algebra system CoCoALib [8]. In the talk we are going to explain these algorithms and give some ideas to improve these algorithms. In addition to that we present some first practical experience which we have made during first computations. Furthermore we report some experiences which we have made when we tried to parallelize these algorithms.

References

[1] A. Grothendieck. Techniques de construction et théorèmes d'existence en géométrie algébrique. IV. Les schémas de Hilbert. In *Séminaire Bourbaki, Vol. 6*, pages Exp. No. 221, 249–276. Soc. Math. France, Paris, 1995.

[2] E. Sernesi. *Deformations of algebraic schemes*, volume 334 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 2006.

[3] R. Hartshorne. Connectedness of the Hilbert scheme. *Inst. Hautes Études Sci. Publ. Math.*, (29):5–48, 1966.

[4] Jerome Brachat, Paolo Lella, Bernard Mourrain, and Margherita Roggero, *Extensors and the Hilbert scheme*, Annali della Scuola Normale Superiore di Pisa, Classe di Scienze (2015), Article in Press, doi:10.2422/2036-2145.201407_003.

[5] Mathias Lederer, *Gröbner strata in the Hilbert scheme of points*, J. Commut. Algebra **3** (2011), no. 3, 349–404.

[6] C. Bertone, P. Lella and M. Roggero. A Borel open cover of the Hilbert scheme. *J. Symbolic Comput.*, 53:119–135, 2013.

[7] F. Cioffi and M. Roggero. Flat families by strongly stable ideals and a generalization of Gröbner bases. *J. Symbolic Comput.*, 46(9):1070–1084, 2011.

[8] Abbott, J., Bigatti, A.: CoCoALib: a C++ library for doing computations in commutative algebra (2016), `http://cocoa.dima.unige.it/cocoalib`

Nœther Normalization and Involutive Bases

Amir Hashemi

Department of Mathematical Sciences, Isfahan University of Technology, Isfahan, 84156-83111, Iran and
School of Mathematics, Institute for Research in Fundamental Sciences (IPM), Tehran, P.O.Box: 19395-5746, Iran
Amir.Hashemi@cc.iut.ac.ir

In this talk, we present a relationship between Nœther normalization and involutive bases. Based on a new definition of Nœther position called *D-quasi stability* [1] we present an efficient algorithm based on the algorithm described by Seiler in [2] (to transform an ideal into quasi stable position) to find, for a given homogeneous ideal, a linear change of variables which transforms the ideal into Nœther position. For this purpose, the type of linear changes we apply is the elementary linear changes, i.e. at each iteration we make a linear change of the form $x_k \mapsto x_k + ax_\ell$ where the pair (x_k, x_ℓ) presents an obstacle for being in Nœther position and a is a random number. We have implemented the described algorithm in MAPLE and illustrate its efficiency via a set of benchmark polynomials. In this direction, we shall mention the work [3] due to Robertz in which he applied the cone decomposition of the given ideal using Janet division to obtain also an sparse linear change of variables for the Nœther normalization. Remark that the criterion to get Nœther normalization described in [3] is *not* equivalent to Nœther position, however, our new criterion is equivalent and this may lead to achieve a more sparse linear change of variables.

References

[1] Hashemi A.: Effective computation of radical of ideals and its application to invariant theory. International Congress on Mathematical Software (ICMS 2014), Seoul, Korea, 2014. *Lecture Notes in Computer Science*, Volume 8592, pages 382–389, 2014.

[2] Seiler, W.M.: A combinatorial approach to involution and δ-regularity II: Structure analysis of polynomial modules with Pommaret bases. *Appl. Alg. Eng. Comm. Comp.* **20**, pages 261–338, 2009.

[3] Robertz, D.: Noether normalization guided by monomial cone decompositions. *J. of Sym. Comput.* **44**(10), pages 1359–1373, 2009.

Divided-difference equation and three-term recurrence relations of some systems of bivariate q-orthogonal polynomials

D.D. Tcheutia[1], M. Foupouagnigni[2], I. Area[3], E. Godoy[4], Y. Guemo Teffo[5]

[1] *University of Kassel, duvtcheutia@yahoo.fr*
[2] *African Institute for Mathematical Sciences, Limbé, Cameroon, foupouagnigni@gmail.com*
[3] *Departamento de Matemática Aplicada II, E.E. Telecomunicación, Universidade de Vigo, Campus Lagoas-Marcosende, 36310 Vigo, Spain, area@uvigo.es*
[4] *Departamento de Matemática Aplicada II, E.E. Industrial, Universidade de Vigo, Campus Lagoas-Marcosende, 36310 Vigo, Spain, egodoy@dma.uvigo.es*
[5] *University of Yaoundé I, guemoyves2000@yahoo.fr*

In this work, partial divided-difference equations and three-term recurrence relations satisfied by the bivariate Askey-Wilson and the bivariate q-Racah polynomials are computed. By using limiting processes, partial divided-difference equations and three-term recurrence relations are also provided for each of the following families of orthogonal polynomials: the bivariate continuous dual q-Hahn, the bivariate Al-Salam-Chihara, the bivariate continuous q-Hahn, the bivariate q-Hahn, the bivariate dual q-Hahn, the bivariate q-Krawtchouk, the bivariate q-Meixner, and the bivariate q-Charlier polynomials. We obtain our results which are all new using mainly the `qsimpcomb` algorithm implemented in Maple in the package `qsum.mpl`.

Linear partial divided-difference equation satisfied by multivariate orthogonal polynomials on quadratic lattices

D.D. Tcheutia[1], Y. Guemo Teffo[2], M. Foupouagnigni[3], E. Godoy[4], I. Area[5]

[1] *African Institute for Mathematical Sciences, Limbé, Cameroon, duvtcheutia@yahoo.fr*
[2] *University of Yaoundé I, guemoyves2000@yahoo.fr*
[3] *African Institute for Mathematical Sciences, Limbé, Cameroon, foupouagnigni@gmail.com*
[4] *Departamento de Matemática Aplicada II, E.E. Industrial, Universidade de Vigo, Campus Lagoas-Marcosende, 36310 Vigo, Spain, egodoy@dma.uvigo.es*
[5] *Departamento de Matemática Aplicada II, E.E. Telecomunicación, Universidade de Vigo, Campus Lagoas-Marcosende, 36310 Vigo, Spain, area@uvigo.es*

In this work, fourth-order partial divided-difference equations satisfied by the bivariate Racah and the bivariate Wilson polynomials are derived. From our result, we recover the difference equation satisfied by the bivariate Racah polynomials given by J.S. Geronimo and P. Iliev. Moreover, we make a conjecture on the form of the partial divided-difference equation satisfied by any multivariate Racah or Wilson polynomials. To illustrate this conjecture, we consider the case of the trivariate continuous Hahn polynomials.

Efficient computation of the bivariate chromatic polynomial for special graphs

M. Gerling[1]

[1] *University of Kassel, Germany, melanie.gerling@mathematik.uni-kassel.de*

In 2003 Dohmen, Pönitz and Tittmann introduced a bivariate generalization $P(G;x,y)$ of the chromatic polynomial $P(G;y)$. While the definition of the usual chromatic polynomial strictly claimes, respectively, different colours for pairwise non-adjacent vertices, the bivariate polynomial expands this set of colours by another set without any restrictions. Let $X = Y \cup Z$ with $Y \cap Z = \emptyset$ be the set of all available colours with $|X| = x$ and $|Y| = y$. By a generalized proper colouring of G we denote a map $\phi : V \to X$ such that for all edges $\{u,v\} \in E$ with $\phi(u) \in Y$ and $\phi(v) \in Y$ $\phi(u) \neq \phi(v)$ holds. In other words two adjacent vertices may only be coloured in the same colour, if this is chosen from Z.

The computation of the chromatic polynomial of a graph is an NP-complete problem. Consequently, this is also valid for the bivariate generalization of the chromatic polynomial. A recursion formula, which was introduced by Averbouch, Godlin and Makowsky in 2008, has exponential complexity. Hence, our aim is to find efficient algorithms or formulas for the calculation of the bivariate chromatic polynomial for special types of graphs. The following results will be presented.

We introduce partition formulas, which can be used to compute the bivariate chromatic polynomial for arbitrary graphs. These formulas are very complex, but they are also an easy method to prove more special but less complex formulas.

Some of those less complex methods are recursion-free equations for the complete partite graphs $K_{2,\ldots,2}$ and $K_{3,\ldots,3}$ as well as a recursion formula for the more general complete partite graph $K_{n_1,\ldots,n_t}$ with $t \geq 1$ and $n_i \geq 1$ for all $i \in \{1,\ldots,t\}$.

Finally, we will consider complete seperators in graphs. In the univarate case, a complete seperator allows a simplification of the computation of the univariate chromatic polynomial. We will show that this is much more difficult in the bivariate case.

References

[1] I. Averbouch, B. Godlin and J. A. Makowsky, *A most general edge elimination polynomial*, in *Graph-Theoretic Concepts in Computer Science*, Lecture Notes in Comput. Sci. **5344**, pp.31-42 (2008). `http://link.springer.com/chapter/10.1007%2F978-3-540-92248-3_4`

[2] K. Dohmen, A. Pönitz and P. Tittmann, *A new two-variable generalization of the chromatic polynomial*, Discrete Math. Theor. Comput. Sci. **6**, pp. 69-90 (2003). http://www.emis.de/journals/DMTCS/volumes/abstracts/dm060106.abs.html

[3] M. Gerling, *Eigenschaften chromatischer Polynome*, Dissertation, Universität Kassel. https://kobra.bibliothek.uni-kassel.de/handle/urn:nbn:de:hebis:34-2015110249265

Index